EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
EUROPEAN BANKING FEDERATION

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
Athough the Guide is aimed at providing supervisory expectations on existing legislative obligations (e.g. under DORA), in some areas it seems to go beyond existing legal requirements. Considering the complexity of the current legislative and regulatory framework for cybersecurity and resilience, the introduction of DORA has been welcomed by banks as a major step towards harmonisation and consolidation of related requirements included in both horizontal legislation and sector-specific policies. It is therefore essential that the Guide is clearly aligned with DORA and avoids introducing additional requirements which do not exist in the Regulation. Consistency and coherence between DORA and the ECB Guide are necessary to ensure smooth implementation and enhanced cyber resilience. Moreover, we would appreciate confirmation that (a) non-banking entities that are out of the perimeter of prudential consolidation, and (b) banks outside the EU, are out of the scope of this Guide. Among the detailed comments we submit, we note especially the following provision and its far-reaching impact: "The organization must retain the ability to bring data and applications back on premises". We propose the deletion of this provision as it would call for duplicating innovation investments (banks would need to maintain the same capabilities on-prem and on the cloud), which would not be sustainable financially and would eventually call into question the benefits of using the cloud. This concern is especially true for SaaS solutions, where scalability would be considerably hindered. In accordance with DORA, financial entities already identify alternative solutions and develop transition plans in a flexible manner; namely either securely transfer contractually obligatory services and related data from third-party ICT service providers in their entirety to alternative providers or alternatively reintegrate them internally. This tailored-business flexibility of DORA under we seek to underline. In addition, some of the suggested practices for pre-outsourcing analysis appear to be quite detailed. Introducing very specific evaluation elements could complicate the initial verification process. Generally speaking, a number of requirements on pre-outsourcing analysis, tests etc., may be challenging to implement as banks' compliance with them would depend on providers' willingness to provide the relevant data. In this respect, leveraging the oversight of CTPPs provided by DORA would be welcome and supportive of banks' efforts to comply. The EBF stands ready to provide any necessary clarifications on all our proposed amendments.

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. Introduction 1.1. Purpose	1.1	1	Amendment	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 should provide flexible and risk-based guidance, rather than prescriptive expectations. This will allow FEs to adapt their risk management frameworks to any cloud-specific or evolving technology risks.	EBF	Don't Publish
	1. Introduction 1.1. Purpose	1.1	2	Clarification	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".	If the intended meaning does not differ between the two, we suggest continuing using the existing definition under DORA.		Don't Publish
	1. Introduction 1.1. Purpose	1.1	2	Clarification	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).	If SaaS is in scope, we seek clarification if the Guide expects Financial Entities (hereinafter: FEs) to have full visibility of each cloud region topology (for example 3 different campus) supporting the SaaS.		Don't Publish
	1. Introduction 1.2 Scope and Effect	1.2	3	Amendment	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.	Ensure that what is requested is feasible / not too burdensome for banks		Don't Publish
	1. Introduction 1.2 Scope and Effect		3	Amendment	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.	We argue for a consistent application of proportionality as well as a risk-based approach. Otherwise, the supervisory expectations in the Guide could be interpreted as applying to a very expansive scope of Cloud Service Providers and their subcontractors.		Don't Publish
	1. Introduction 1.2 Scope and Effect		3	Amendment	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. 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".	The current wording is tantamount to broadening the scope of application provided for by DORA, which is aimed solely at providers supplying an ICT service (in particular cloud providers). Here, the fact that a non-CSP third party does or does not provide an ICT service is not taken into account. Is the SSC necessary for the provision of the service rendered by the non-SSC TP or does the non-SSC TP call on a SSC for its internal management unrelated to the service provided?		Don't Publish
	1. Introduction 1.2 Scope and Effect		2	Clarification	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 Guide also broadens the scope of the term 'outsourcing' in that it is used interchangeably with 'purchase of'. It should be noted that DORA does not use the term 'outsourcing' but rather the term 'purchase of ICT services,' which is a more suitable expression for the Guide.			Don't Publish
	1. Introduction 1.2 Scope and Effect		3	Clarification	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).	In order to avoid uncertainity regarding the scope of application.		Don't Publish
	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	"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.	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.		Don't Publish
	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis			Amendment	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* ".	In order to ensure that what is requested is feasible and based on proportionality criteria.		Don't Publish

	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		4 & 5	Amendment	□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.	It would not be feasible to assess some of the risk considerations at the pre-contractual stage. Some of the risk considerations lack clarity or are too subjective.		Don't Publish
	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		4	Clarification	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.			Don't Publish
	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		5	Clarification	The reference to the risks of a multi-tenant environment is not clear. Cloud Services are multi-tenant by design.	In order to provide certainty and avoid misunderstandings.		Don't Publish
	Chapter 2.1 Governance of Cloud Services 2.1.3. Consistency between an institution's cloud strategy and its overall strategy	2.1.3	5	Clarification	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	In order to avoid misalignment with DORA provisions.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		6	Clarification	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.	Our counter-proposal to that provision would be tailored-business continuity plans to the specific risks and capacities of the institution, focusing on practical and feasible measures.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		6	Amendment	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 ECB guide is not meant to be a legislative framework, it should not define requirements, also considering similar existing regulatory requirements (e.g. DORA, etc.). It is important to avoid requirements proliferation which results in uncertainty		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		6	Clarification	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).	There seems to be in certain cases some ambiguity on whether back-up is required not only for data but also 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		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		6	Amendment	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 ECB guide is not meant to be a legislative framework, it should not define requirements, also considering similar existing regulatory requirements (e.g. DORA, etc.). It is important to avoid requirements proliferation which results in uncertainty.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions				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).			Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		6	Deletion	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)".	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 entail significant operational and maintenance costs. Business continuity management (BCM) must address scenarios where the cloud provider can assist in recovering from service downtime. In other scenarios, member states should have mechanisms to place the service under their administration in the event of unavailability, as it happens for other utilities such as electricity. For CSPs, it is necessary to implement similar resolution mechanisms that ensure the availability and integrity of services and data.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		6	Amendment	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".			Don't Publish

	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		6	Clarification	With reference to the request *"appropriate cloud resilience measures"*, confirmation is sought that this provision is applicable only with reference to IaaS Clouds.	In order to avoid misinterpretation and ambiguity.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		7	Deletion	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 order to avoid misinterpretation and ambiguity.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		6 & 7	Deletion	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***".			Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Deletion	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* ".	We recommend more flexible backup strategies that consider both cost and risk, allowing financial entities to balance operational efficiency with data security. In accordance with DORA, financial entities already identify alternative solutions and accordingly develop transition plans in order to either securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		7	Amendment	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"* .	In order to ensure that what is requested is operationally feasible for banks.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		8	Amendment	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"*	Ensure that what is requested is feasible / not too burdensome for banks		Don't Publish
	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		7	Amendment	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*)".			Don't Publish
	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		7	Amendment	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"*.			Don't Publish
	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	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* "			Don't Publish
	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		7	Clarification	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.	This comment is meant to better identify an actionable role of the institution within joint a test on CSP' proprietary infrastructure,		Don't Publish
	Chapter 2.2 Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	2.2.3	7 & 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 Business Continuity Plan (BCP) testing should be addressed in the BCP plan, and the control environment of the CSP. Such suggested guidance is carrying risks of creating an undesirable environment of continual off-cycle contract renegotiations without meaningfully addressing the real issue or risk.		Don't Publish
	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		7	Deletion	"*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* ."	It is unrealistic to be able to perform the tests "***at short notice***". We would suggest deleting "*short notice* ". Also we would suggest removing "*should not rely exclusively on relevant disaster recovery certifications* " and clarifying in which area certifications are not valid, taking into account the criteria of essentiality and criticality.		Don't Publish
	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		7	Amendment	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 even* t."	In order to ensure what is requested is operationally feasible for banks.		Don't Publish
	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		7	Amendment	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".*	In order to ensure what is requested is operationally feasible for banks.		Don't Publish

	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		7	Clarification	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.	In order to avoid misinterpretation and ambiguity.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Deletion	The concentration assessments cannot be carried out by single institutions, such assessment can be performend only in a centralised manner (i.e. via a joint assessment coordinated by the ECB). This provision should therefore be **deleted**.	The Financial Entities (FEs) don't have the aggregated information necessary to perform concentration assessments. Such an assessment should be carried out by European Institutions. 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.		Don't Publish
	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks		8	Clarification	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.	Ensure what is requested is operationally feasible for banks.		Don't Publish
	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 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.	We would suggest deleting the last sentence in 2.2.4, given that new functions are difficult to be taken into account at the moment of an evaluation of concentration risk.		Don't Publish
	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and cryptographic key management processes	2.3	9	Amendment	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."	It is important to avoid requirements proliferation which results in uncertainty		Don't Publish
	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 statement regarding data location restriction is a good practice, it should be specified that it's a suggestion and not an obligation	It is important to avoid requirements proliferation which results in uncertainty		Don't Publish
	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	Clarification	With reference to envisaged "*good practice for i*nstitutions *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 shoud this aspect be weighted against considerations of geographical concentration.	To avoid misinterpretation and ambiguity		Don't Publish
	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and cryptographic key management processes	2.3.1	9	Amendment	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".	t is important to avoid requirements proliferation which results in uncertainty		Don't Publish
	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		10	Clarification	*"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.	To avoid misinterpretation and ambiguity		Don't Publish
	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data	2.3.2	10	Amendment	The statement regarding acceptable countries list in terms of data processing locations is not acceptable, such a list must be defined by regulators	It's important to agree on responsibilities, financial entities don't have the standing to define a list of acceptable countries in terms of data processing. It shoud be defined by European regulators or authirities.		Don't Publish
	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data		10	Amendment	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 guide is not meant to be a legislative framework, it should not define requirements (or soft requirements), also considering similar existing regulatory requirements (e.g. DORA, etc.). It is important to avoid requirements proliferation which results in uncertainty		Don't Publish
	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	2.3.3	10	Amendment	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 ECB guide is not meant to be a legislative framework, it should not define requirements, also considering similar existing regulatory requirements (e.g. DORA, etc.). It is important to avoid requirements proliferation which results in uncertainty		Don't Publish
	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	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."*	To avoid misinterpretation and ambiguity		Don't Publish
	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	Amendment	*"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"*	The amdendment is aimed at getting sense to the provision since the negotiation phase of contractual clauses precedes the configuration of the cloud environment		Don't Publish
	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements		11	Clarification	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)	Clarification on perimeter of roles and responsibilites regarding IAM		Don't Publish
	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	2.3.4.2	11	Amendment	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	Ensure that what is requested is feasible / not too burdensome for banks		Don't Publish
	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4	12	Clarification	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."* c larification is needed with respect to the meaning of "*principle-based"*.	To avoid misinterpretation and ambiguity		Don't Publish
	2.4 Exit strategy and termination rights 2.4.1 Termination rights		12	Amendment	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"*.			Don't Publish

	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Amendment	Regarding 2.4.1 paragraph (2) describing other changes that could also lead to such a reason for termination, including in particular: (iv) relocation of the data center... and (vi) a change in the regulations applicable to data location and data processing ... With reference to the sentence "(vii) s*ignificant changes to the management of cybersecurity risk in the chain of sub-contractors* ", we suggest an amendment by generalising the requirement as follows: "(vii) *violation of the cybersecurity obligations indicated in the contractual clauses, also with reference to the chain of sub-contractors* ".	We suggest adding "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.		Don't Publish
	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Amendment	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* "	To include all the security measure that the CSP has to adopt		Don't Publish
	2.4 Exit strategy and termination rights 2.4.1 Termination rights		12	Amendment	*"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.	To avoid misinterpretation and ambiguity		Don't Publish
	2.4 Exit strategy and termination rights 2.4.1 Termination rights		12	Deletion	The statement regarding termination right seems to be a brand new requirement we propose to remove the chapter "2.4.1 Termination rights" considering that many aspects are in overlap with other regulations. We need clarification on what does "*an excessive increase* " means in "(iii) *an excessive increase in expenses under the contractual arrangements that are attributable to the CSP* ".	The ECB guide is not meant to be a legislative framework, it should not define requirements, also considering similar existing regulatory requirements (e.g. DORA, etc.). It is important to avoid requirements proliferation which results in uncertainty.This section is also a broad interpretation of Article 28 (7) of DORA. Some of the remediation cases are impossible to obtain. Therefore, we would suggest amending or clarifying the sentence.		Don't Publish
	2.4 Exit strategy and termination rights 2.4.2 Components of the exit strategy and alignment with the exit plan	2.4.2	13	Deletion	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 .*	Article 28 (8) of 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 including a timeline, which corresponds to the exit and termination conditions.		Don't Publish
	2.4 Exit strategy and termination rights 2.4.3 Granularity of exit plans	2.4.3	14	Deletion	The statement regarding detail leveles of exit plans seems to be a requirement (with regard to critical milestones, skill sets, etc.). We propose to remove the chapter "*2.4.3 Granularity of exit plans* " considering that many aspects are in overlap with other regulations.	The ECB guide is not meant to be a legislative framework, it should not define requirements, while taking into consideration that there are similar existing regulatory requirements (e.g. DORA, etc.) in placec. Thereore, it is essential to avoid requirements proliferation, which results in uncertainty.		Don't Publish
	2.4 Exit strategy and termination rights 2.4.3 Granularity of exit plans	2.4.3	14	Amendment	If our proposal to delete the chapter "*2.4.3 Granularity of exit 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*** *)."*	Since the Guide specifies the possibility of taking into account external support, this provision 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. Therefore, it should be also 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 maintaining the alignment with relevant provisions of the Data Act.		Don't Publish
	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	2.4.4	14	Deletion	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)". This requirement is quite impossibile 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, matain 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."	Ensure that what is requested is feasible / not too burdensome for banks		Don't Publish
	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	2.4.4	14	Deletion	"*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.			Don't Publish
	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	2.4.4	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.			Don't Publish
	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5	15	Amendment	"*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.	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.		Don't Publish

	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5.1	15	Clarification	*"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.	In order to avoid misinterpretation and ambiguity.		Don't Publish
	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5.1	15	Clarification	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.			Don't Publish
	2.5 Oversight, monitoring and internal audits 2.5.3 Contractual Clauses	2.5.3	15	Deletion	*"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.	This recommendation does not reflect how contractual negotiations with CSPs actually occur and it will not be practically feasible to achieve. Standard contractual clauses might limit the ability of the industry to embrace technological advancements, they might also hinder the ability of institutions to negotiate effectively with their providers and are not effective in an innovative space unless being regularly updated. Any standard contractual clauses should be set out as indicative examples with no requirement for rigid adherence.		Don't Publish
	2.5 Oversight, monitoring and internal audits 2.5.3 Contractual Clauses	2.5.3	16	Deletion	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."*	This seems to represent an additional requirement		Don't Publish
	2.5 Oversight, monitoring and internal audits 2.5.3 Contractual Clauses	2.5.3	16	Clarification	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.	Better clarify the expectations for the recommendations to use standard clauses developed by public authorities.		Don't Publish