EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company

ABI - ITALIAN BANKING ASSOCIATION

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

In general, although the Guide is aimed at providing guidance on existing regulatory obligations, it seems that some of the indications may actually imply new requirements, on top of the current regulatory framework, which is already very complex, considering various regulations such as DORA, EBA Guidelines on outsourcing, and EBA Guidelines on IT risk.
In this regard, the role of possible guidance by the NCAs should be clarified (i.e. whether it is assumed to be addressed to LSI only or also to SI further to this ECB Guide). Also, the perimeter of the entities in-scope should be clarified (more precisely, we would seek 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).
A particularly impactful provision is the following: "The organization must retain the ability to bring data and applications back on premises". This approach is deemed excessively limiting, especially concerning the use of SaaS solutions, which could hinder the scalability and elasticity of institutions. In accordance with DORA, financial entities already identify alternative solutions and develop transition plans 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.
Moreover, some of the suggested practices for pre-outsourcing analysis appear to be quite detailed, introducing very specific evaluation elements. This could complicate the initial verification process. Generally speaking, many requirements identified in the draft Guide, as regards pre-outsourcing analysis, tests etc., appear very challenging as the actual ability for the bank to comply depends on providers' willingness. Banks should be given levers to obtain compliance from providers.

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	Personal data
1	1. Introduction 1.1. Purpose	1.1	2	Clarification	The ECB's definition of critical or important functions reported in the section "Definitions of terms for the purposes of this Guide" is: *"Activities, services or operations whose discontinuance is likely to lead to disruptions of services that are essential to the real economy in one or more member states or the disruption of financial stability, given the size, market share, external and internal interconnectedness, complexity or cross border nature of an institution or group's activities, particularly as regards the substitutability of those activities, services or operations."* It should be confirmed that for the purposes of this Guide, critical functions are only those from which systemic impacts may arise	To avoid misinterpretation and ambiguity	Don't Publish
2	1. Introduction 1.1. Purpose	1.1	2	Amendment	"For the purposes of this Guide, it should be confirmed that critical and important functions within scope should be limited to only those functions from which systemic impacts may arise, in line with the ECB's definition reported in the section "Definitions of terms for the purposes of this Guide".	Clarify applicability of expectations for backup of critcal or important systems hosted by CSP's	Don't Publish
3	1. Introduction 1.1. Purpose	1.1	2	Amendment	The use of the word "undertaking" in the definitions of private and community cloud is inconsistent with the definitions provided in the Guidelines for Outsourcing Arrangements and in those commonly used (e.g. from NIST). It should be substituted with "business", "enterprise" or "institution" to avoid uncertainty in the definitions.	To avoid misinterpretation and ambiguity	Don't Publish
4	1. Introduction 1.1. Purpose	1.1	2	Amendment	Alignment of the definition of "ICT asset" to the definition contained in DORA is highly recommended: "a software or hardware asset in the network and information systems used by the financial entity".	To avoid misinterpretation and ambiguity	Don't Publish
5	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
6	1. Introduction 1.2 Scope and Effect	1.2	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).	To avoid uncertainity regarding the scope of application	Don't Publish
7	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 request about the level of diligence regarding risk management, processes, and controls seems more far reaching than regulation. The sentence *"Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls."* should be modified as follows: *"Consequently, Institutions should assess that their CSPs have established equivalent risk management practices, processes and controls."* . Clarification would be useful on what "equivalent" means in practice.	Ensure that what is requested is feasible / not too burdensome for banks	Don't Publish
8	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Amendment	The sentence "*ensure the CSP has properly implemented relevant checks* ," should be modified as follow: "*assess that the CSP has properly implemented relevant checks,"*	Ensure that what is requested is feasible and based on proportionality criteria	Don't Publish
9	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Clarification	The reference to the risks of a multi-tenant environment is not clear. Cloud Services are multi-tenant by design.	To provide certainty and avoid misunderstandings	Don't Publish
10	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	To avoid misalignment with DORA Provisions	Don't Publish
11	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.1	6	Clarification	This provision could implicitly introduce new requirements, while referring to the concept of a Holistic Perspective. Whenever the expectation is to consider both Business Continuity (Backup/Restore) and Exit Strategy elements in a unique framework, we foresee a potential risk in a dramatic increase in complexity, significantly limiting the architectural alternatives to be considered and further complicating the verification and control actions towards CSPs. There seems also to be in certain cases some ambiguity about whether backup is required for data only or for systems (which is completely different in terms of impact). In particular: In the first part of the paragraph the focus is on data while in the following part the backup procedure involve also critical or important systems.	Clarification on aspects regarding Business Continuity and Exit Strategy	Don't Publish
12	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 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

13	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 suggestion that back-ups of Critical or Important Functions should not be stored in the cloud which hosts the services will not always be practically possible or in the best interests of the institution and its resilience. In addition many initiatives that have been deployed in the cloud could be significantly impacted by this requirement The guide indicates that *"back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned"* . In our understanding the backups could reside on a different network architecture (physically and logically segregated from the source ICT system), even if it belongs to the same CSP, and not necessarily be implemented on a completely different CSP. Please note that the measure to have back-ups stored in other cloud providers seems to be not applicable for SaaS Cloud and in any case would imply a huge effort with direct impact on the cloud benefits. In addition, it should be noted that the CSP ensures the Business Continuity through redundancy not through a backup system and that the article 12 of DORA refers in general to TPP (not specific to CSP). We would propose that instead of prohibiting the use of the same cloud for backups, the ECB should require institutions to assess the resilience of their backups based on the risk associated with the services provided, accordingly art. 12,(3) of DORA (e.g. "When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system").	Ensure that what is requested is feasible / not too burdensome for banks	Don't Publish
14	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	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 impossibile 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, 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
15	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	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".	To avoid misinterpretation and ambiguity	Don't Publish
16	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 statement regarding virtual machine-based applications and containerisation development seems to exclude SaaS solutions	To avoid misinterpretation and ambiguity	Don't Publish
17	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	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	To avoid misinterpretation and ambiguity	Don't Publish
18	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 Guide in this chapter refers to the EBA guidelines in footnote 7 to define critical functions. Deletion of this reference is suggested, to maintain consistency with the definitions provided in the table "*Definitions of terms for the purposes of this Guide* " on page 2.	To avoid misinterpretation and ambiguity	Don't Publish
19	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 ECB consultation document as proposed makes the use of cloud solutions difficult or even impossible, making it not economically sustainable and/or not feasible. ECB wants banks to be "responsible" for the solutions they adopt, and this is correct in principle, but then the written policies require that banks have "instant" internal recovery capabilities of what is managed in the cloud or "switch" , always instant, on another provider. This is practically not possible because: • If you should have a "ready-to-use" internal solution, the costs are doubled and, in that case, you'd better use the internal capabilities without using the cloud; on the other hand, a "ready-to-use" solution is not always possible • Instant switching to another provider, in addition to increasing costs (probably making the cloud uncompetitive), is not always possible The expectation "*The institution must maintain the ability to bring data and applications back on-premises* " is overly limiting - especially when it comes to the use of SaaS solutions - and could hinder the scalability of solutions and the adaptability/flexibility of the institutions themselves. It should also be emphasised that DORA fully regulates exit strategies, requiring financial institutions to identify alternative solutions and develop transition plans to securely transfer contractually obligated services and related data from third-party ICT service providers in their entirety to alternative providers or reintegrate them internally. These regulatory provisions leave financial institutions the margin of choice based on concrete situations. The phrase "The institution must maintain the ability to bring data and applications back on-premises" should be deleted or alternatively reworded in line with the regulatory provisions as follows: "*The institution must maintain the ability to bring data and applications back on-premises or transfer them to alternative CSPs or back-up providers* ".	Ensure that what is requested is feasible / not too burdensome for banks. Moving services to another CSP should be considered as a valid alternative for business continuity	Don't Publish
20	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	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 follow:* *"When conducting disaster recovery tests with the CSP, the institution, where possible, may perform spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event"*	Ensure that what is requested is feasible / not too burdensome for banks	Don't Publish
21	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	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 follow *"In relation to critical services outsourced, if joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution"*	Ensure that what is requested is feasible / not too burdensome for banks	Don't Publish
22	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	2.2.3	7	Amendment	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)"	Ensure that what is requested is feasible / not too burdensome for banks	Don't Publish
23	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	2.2.3	7	Amendment	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"	Ensure that what is requested is feasible / not too burdensome for banks	Don't Publish
24	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	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"	Ensure that what is requested is feasible / not too burdensome for banks	Don't Publish
25	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	2.2.3	7	Clarification	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

26	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	2.2.3	7	Amendment	*"test disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications"* should be modified as follow: *"with reference to IasS Cloud test disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications"*	Ensure that what is requested is feasible / not too burdensome for banks	Don't Publish
27	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	2.2.3	7	Clarification	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.	To avoid misinterpretation and ambiguity	Don't Publish
28	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Amendment	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 institutions don't have the aggregated information necessary to perform concentration assessments. Such an assessment should be carried out by european institutions	Don't Publish
29	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Clarification	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 that what is requested is feasible / not too burdensome for banks	Don't Publish
30	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
31	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 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
32	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	Clarification	With reference to envisaged "*good practice for institutions to restrict the locations where CSPs can store their data"* it has to be noted that when dealing directly with a CSP - as opposed to a TPP - the location is usually an institution's own choice. It should be clarified how shoud this aspect be weighted against considerations of geographical concentration.	To avoid misinterpretation and ambiguity	Don't Publish
33	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
34	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	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
35	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
36	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 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
37	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
38	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	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
39	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	Clarification	A definition of Outsourced Asset is required: the Guidelines on Outsourcing cover the outsourcing of "processes" or "functions", it is unclear what cloud service would constitute an asset, what would be considered different assets of the same kind or different types of assets, especially regarding the adoption of SaaS products or that of serverless services	To avoid misinterpretation and ambiguity	Don't Publish
40	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
41	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	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
42	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

43	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."* clarification is needed with respect to the meaning of "principle-based"	To avoid misinterpretation and ambiguity	Don't Publish
44	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4	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"	Ensure that what is requested is feasible / not too burdensome for banks	Don't Publish
45	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
46	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	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
47	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Amendment	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	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
48	2.4 Exit strategy and termination rights 2.4.3 Granularity of exit plans	2.4.3	14	Amendment	The statement regarding detail leveles of exit plans seems to be a requirement (wrt 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, also considering similar existing regulatory requirements (e.g. DORA, etc.). It is important to avoid requirements proliferation which results in uncertainty	Don't Publish
49	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
50	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 to better clarify what are the CSP's performance that should be monitored independently and limiting to cases in which the institution has reason to believe manipulation can occur	To avoid misinterpretation and ambiguity	Don't Publish
51	2.5 Oversight, monitoring and internal audits 2.5.3 Contractual Clauses	2.5.3	16	Amendment	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
52	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's timeline	Better clarify the expectations for the recommendations to use standard clauses developed by public authorities	Don't Publish