EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company

ECUC

Contact person

Mr/Ms

First name

Surname

Email address

Telephone number

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

General comments

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

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

Deadline:	15.07.2024

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
1	1. Introduction 1.1. Purpose	1.1	2	Amendment	The guide is using the BRRD (Bank Recovery and Resolution Directive) definition of critical and important functions (CIFs), rather than the DORA definition or other set definition from NIS2 or EBA guidelines which are understood to be different. Neither is any reference made to the EBA Guidelines on outsourcing, guidelines that use concepts that are also different from this ECB Guide.	It is expected that the guide uses DORA definitions, and also clarifies how the current EBA Guidelines should be applied in relation to IT and/or cloud outsourcing. A different definition will lead to inconsistent regulatory context.		Don't publish
2	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Clarification	Without clarity that this relates to cloud services supporting CIFs, the guide will be lacking in proportionality and feasibility. Additionally, without clarification as to the type of cloud service subject to specific requirements, there are certain expectations which are not even practically possible for e.g. contractual obligations in pre-outsourcing analysis	In general, an opening statement that a risk- and proportionality-based approach is possible regarding CIF and non-CIF and type of cloud services is missing in comparison to DORA. In some articles the proportionality approach has been addressed, while in other articles this approach is missing.	,	Don't publish
3	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Clarification	There is a lack of clarity over how far down the supply chain the requirements should apply. It should be limited to direct cloud services, with which the FI has a contractual relationship.	Clarification on the outsourcing chain is required.	,	Don't publish
4	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	4	Clarification	The only way that an FI can enforce a complete answer to any of suggested requirements in Pre-outsourcing analysis is via a contract, yet this provision is aimed at the pre-contractual phase. Could you please clarify the expectation?	Clarification in regards to good practice is required.	,	Don't publish

5	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.1	6	Amendment	The ECB understands that business continuity management (BCM) measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the FI has to perform an exit under stress or an exit without cooperation from the CSP(s) whereas we suggest we should address severe but plausible scenarios, as worst-case scenarios are highly unlikely and subjective. Also, exit under stress is not necessarily required and exit should be done only after assessing the circumstances. The lack of proportionality in not limiting Exiting under stress requirements to only services supporting CIFs is stretching the feasibility of the guidance. We suggest to maintain the approach laid out in 2.4.2 where business continuity management and exit management are not the same. The (partial) unavailability of relevant cloud services is in our understanding a temporary scenario and not equal to an exit scenario which will terminate the business relationship with a CSP.	In general, an opening statement that a risk- and proportionality-based approach is possible regarding CIF and non-CIF and type of cloud services is missing in comparison to DORA and the EBA Guidelines on outsourcing. In some articles the proportionality approach has been addressed, while in other articles this approach is missing. Exiting under stress described in 2.2.1 does not seem to be in line with the definition of exit strategy and plan in 2.4.2.: "*While BCM measures should ensure the continuity of services in the short term, exit plans should ensure continuity in the long term.*" Clarification in this reqard is required.	,	Don't publish
6	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	6	Clarification	Certain requirements relating to having on-premise solutions for CIFs or having multiple CSPs for a service may not be necessarily feasible and practical to implement as it does not address the risk posed instead leads to different concentration risk. 'The institution must retain the ability to bring data and applications back on-premises'. What is exactly expected? This is a new requirement which is practically not feasible. A strict rule to have a mandatory "back on-premise" ability for each application as part of business continuity or disaster recovery processes is disproportionate and will essentially stop all cloud adoption, as it would require to have all on-prem infrastructure in place at all times. It would also stop all investments in building up back-up capabilities with a 2nd or 3rd CSP and consequently renders the previous bullet void. Our view is that this approach would decrease operational resilience and increase costs. In addition, it is a very far-reaching requirement that does not seem to fit in a world (as supported by the ESA's) in which on-premise solutions are replaced with SAAS and where alternative SAAS providers serve as proper backups. Most Services have never been on premise. Measures like alternative back-up/ providers should be sufficient.	Due to the lack of on-premise definition, this could also exclude the possibility of self-operation in external data centers as well as traditional outsourcings, which ignores today's reality for small and medium-sized enterprises. We ask for clarification and adaptation of the language. e.g.: The institution must retain the ability to operate data and applications in alternative deployment models.	,	Don't publish

7	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	6	Amendment	In order to avoid jeopardising the security of network and information systems, the ECB considers that back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned'. Is it the security or the continuity? In addition: what does this mean in practice? For SAAS solutions primary servers handle live data and backup servers are designed to create and store copies of data from primary servers. This is a far-reaching requirement. What is the real risk that is supposed to be mitigated? Please advise. Does the requirement only address critical or important functions?	In general, an opening statement that a risk- and proportionality-based approach is possible regarding CIF and non-CIF and type of cloud services is missing in comparison to DORA. In some articles the proportionality approach has been addressed, while in other articles this approach is missing.	,	Don't publish
8	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Deletion	Some text is perceived too prescriptive; this will ensure that the guidance quickly becomes out-of-date as practices and technologies rapidly evolve in this space. This occurred with the 2013 MAS Risk Management Regulations. E.g. we recommend deleting: “To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP. For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service solutions” (Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions)	The guide must be embedded within the full regulatory and legislative landscape (Data act, EBA guidelines)	,	Don't publish
9	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	Deletion	"On the basis of these provisions, the ECB understands that an institution should test its CSP’s disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications. When conducting disaster recovery tests with the CSP, the institution should perform spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event." Is it the obligation of the institution to initiate a.o. spot checks? It is suggested to delete the obligation for conducting spot checks as it is considered unrealistic to conduct spot checks by each institution for all services. In all cases a materiality lens should be applied through to follow proportionality principles.	In general, an opening statement that a risk- and proportionality-based approach is possible regarding CIF and non-CIF and type of cloud services is missing in comparison to DORA. In some articles the proportionality approach has been addressed, while in other articles this approach is missing.	,	Don't publish
10	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 assessment provisions fail to take account of the assessments to be undertaken by authorities as part of the incoming Critical Third Party regime. These should be leveraged, rather than expecting assessments on a regular basis by the firm. We suggest to also refer to the EBA guidelines on outsourcing (which should also be part of the supervisory approach of the ECB as long as these guidelines are not revoked or amended – if not; justification should be given why the EBA Guidelines are not taken into account).	The guide must be embedded within the full regulatory and legislative landscape (Data act, EBA guidelines)	,	Don't publish

11	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.5	8	Amendment	The pre-contractual assessment obligated by DORA is the key.The requirement on obliging CSPs to assist with a transition is superfluous given the legal obligations set out within the Data Act. Similarly, the Data Act stipulates 7 months for the transition, which is not reflected in the ECB guidance.	The guide must be embedded within the full regulatory and legislative landscape (Data act, EBA guidelines)	,	Don't publish
12	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Amendment	The prescriptive nature of the guidance on termination rights detracts from the precriptive requirements set out within DORA. The value of the guidance is in supplementing the legal requirements, not proposing alternative criteria.	The guide must be embedded within the full regulatory and legislative landscape (Data act, EBA guidelines)	,	Don't publish
13	1. Introduction 1.2 Scope and Effect	1.2	3	Clarification	The ECB Guide states in the second paragraph of this chapter that it “does not lay down legally binding requirements ... nor should it be construed as introducing new rules or requirements”. However the general wording of the ECB Guide seems to set explicit expectations that in our opinion go beyond the DORA-requirements. In order to avoid misunderstandings, we would welcome a very clear distinction between explicit (binding) expectations on the one hand, and (non-binding) best practices – only clarifying a possible approach – on the other hand. As DORA constitutes lex specialis with regard to NIS 2 (see Recital 16 DORA), we assume that institutions are allowed to implement this ECB Guide according to the proportionality principle in DORA. Please confirm. Besides, Article 21 NIS 2 also includes some proportional approach. Please explain how these principles/approaches in NIS 2 and DORA interrelate and how they can be used by entities, without the risk of conflicting interpretation by the entities. This creates uncertainty and unclarity, please elaborate and advise.	The guide must be embedded within the full regulatory and legislative landscape (Data act, EBA guidelines)	,	Don't publish
14	1. Introduction 1.2 Scope and Effect	1.2	3	Deletion	On the one hand the ECB guide takes EBA guidelines on outsourcing as a starting point and DORA is considered as much as possible. On the other hand, DORA precedes over the other 2. Please clarify if the ECB Guide is meant to reflect that the ECB Guide should be read in conjunction with DORA and EBA Guidelines on outsourcing arrangements and that DORA takes precedence over this ECB Guide or whether its meant to reflect that DORA takes precedence over both this ECB guide and the EBA guidelines on outsourcing arrangements. Wouldn't it be better to bring this guide under DORA instead of seperately?	The guide must be embedded within the full regulatory and legislative landscape (Data act, EBA guidelines)	,	Don't publish
15	1. Introduction 1.2 Scope and Effect	1.2	3	Clarification	ECB states that the Guide does not provide for additional rules, nor that it replaces existing rules. However, in many paragraphs, rules/guidelines are mentioned referring to 'good practice': can you be more specific on the basis of such good practice? Where is that specifically mentioned?	Clarification in regards to good practice is required.	,	Don't publish

16	1. Introduction 1.2 Scope and Effect	1.2	3	Clarification	In relation to the foregoing question, please elaborate more on the binding status of the various requirements as laid down in the Guide; on the one hand it is mentioned that the Guide 'does not lay down legally binding requirements', but on the other hand on various occasions it appears that financial institutions are required to comply to the requirements by using the words 'institutions should', see for instance 2.1.2, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.3.2., 2.3.2., 2.3.4.1., 2.3.4.2., 2.4.1., 2.4.2., 2.4.3., 2.5., 2.5.1., 2.5.2., 2.5.3 and lso the use of the word 'ensure' in the last bullet in 2.2.2.. Is the assumption correct that the words 'should' and 'ensure' imply that there is not strict obligation to comply, but merely imply a non-binding suggestion? Please advice and instruct.	Clarification on the binding status of the various requirementes is required.	,	Don't publish
17	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question	2.1.1	4	Deletion	This governance /responsibility is not new and already part of existing and applicable EU regulatory (DORA, EBA). Advise to delete	The guide must be embedded within the full regulatory and legislative landscape (Data act, EBA guidelines)	,	Don't publish
18	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Clarification	Whilst it is referred to clause 28(4) DORA, various actions are listed for the FE's to perform, partly based on 'good practice', but is is not clear where those actions originate from exactly. Can you please elaborate?	Clarification in regards to good practice is required.	,	Don't publish
19	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Clarification	"Assess whether the institution has the expertise and human resources required to implement and perform these checks;" This is very hard/impossible to check. Please verify how to do that.	Clarification in regards to good practice is required.	,	Don't publish
20	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	Clarify on sentence: when selecting a CSP an institution should ensure that business continuity, resilience and disaster recovery capabilities can be maintained, including for all outsourced cloud services. Is the purpose here focus on entire chain including CoIF and non-CoIF / 4/5th party, orelse? What is the scope of All outsourced cloud services?	Clarification on the outsourcing chain is required.	,	Don't publish
21	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	When considered 'cloud Services' is this then Infrastructure (IaaS), Platform (PaaS), Software (SaaS) or all or/and the strict 'Definition in definition of terms for purpose of this Guide'? Please advise.	Clarification on the scope of the cloud services is required.	,	Don't publish

22	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 title states "Proportionate requirements for critical functions". Advised to change it to critical or important.	The guide should use consistent wording.	,	Don't publish
23	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 measures mentioned to contribute to resilience that can be taken by the institution are mentioned here. However one can read these measures (particulary bullet 1,2) as measures at the vendor. In that case the measure that can be taken by the institution is on the contractual requirements and management. If so, please refer to these type of measures.	The guide should use consistent wording and structure.	,	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	Clarification	If joint tests with the CSP are not possible, the institution should ensure that all affected components within the CSP's area of responsibility are covered by tests conducted by the institution. Could you please advise how this should be achieved?	Clarification in regards to good practice is required.	,	Don't publish
25	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	When assessing concentration risks, three main aspects may be considered: concentration in a specific provider, concentration in a specific geographical location and concentration in a specific functionality/service Question: what is the alternative for functionality concentration. Please provide good practice.	Clarification in regards to good practice is required.	,	Don't publish
26	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	A definition of concentration risk and lock-in risk are not defined / captured. This makes the paragraph difficult to read/scope. Could you please provide a definition and a good practice?	Clarification in regards to good practice is required.	,	Don't publish
27	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Clarification	Can you please explain what is exactly meant with 'an excessive increase in expenses under the contractual arrangements that are atributable to the CSP'? In particular, please explain if and how this differs from a contractual breach and please provide (an) example(s).	Clarification in regards to good practice is required.	,	Don't publish
28	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Clarification	What is meant exactly with (vii) significant changes to the 'management' of cybersecurity risk in the chain of subcontractors? Could you please provide a good practice?	Clarification in regards to good practice is required.	,	Don't publish
29	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Clarification	Whilst it is referred to clause 28(7) DORA, various reasons for termination are listed form (i) tot (ix) but is is not clear where those reasons originate from exactly. Can you please elaborate?	Clarification in regards to good practice is required.	,	Don't publish

30	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question	2.1.1	4	Clarification	"Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls." This is a broad and unspecific requirement. Please clarify how "equivalence" can be sufficiently achieved. While the intention is understood it will be inefficient and potentially ineffective If this is to be ensured by each institution individually.	Clarification in regards to good practice is required.	,	Don't publish
31	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	It is requested to clarify if an "exit without cooperation from the CSP" is relating to a scenario where we observe unwillingness of a CSP to fulfill contractual obligations.	Clarification in regards to good practice is required.	,	Don't publish
32	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Amendment	We suggest to maintain the approach laid out in 2.4.2 where business continuity management and exit management are not the same. The (partial) unavailability of relevant cloud services is in our understanding a temporary scenario and not equal to an exit scenario which will terminate the business relationship with a CSP.	The guide should use consistent wording and structure.	,	Don't publish
33	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	11	Clarification	Could you please clarify what the mentioned "individual clauses" would cover.	Clarification in regards to the guide is required.	,	Don't publish
34	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	2.4.4	15	Clarification	Please clarify if "conflicting legislation" is a scenario that needs to be catered for in case the service provider is an EU company	Clarification in regards to the guide is required.	,	Don't publish