EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company

Nordea Bank Abp

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

We welcome an attempt to add further guidance to cloud outsourcing but see the following main issues which should be addressed in further reviewing and updating the Guide:

- Better alignment with DORA main regulation and accompanying RTS:s including definitions which should be fully aligned between the Guide and DORA
- Retaining proportional approach which is also applied in DORA to reduce complexity and allow for risk-based approach
- Ensure the precedence of DORA at all times and consistently throughout the document
- Due to DORA being lex specialis to NIS2, remove references to NIS2 as DORA is more specific for end-to-end supply chain monitoring and management, including risks and controls

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	Clarification	DORA main regulation EU 2022/2554, together with its regulatory technical standards, especially ITS on the Register of Information, RTS for ICT services supporting critical or important functions and RTS for subcontracting, are already detailed and specific on how financial enitites should manage its end-to-end supplier value chains, including cloud. This guide should refer to DORA main regulation and the more detailed RTS:s at all times and accurately, especially as DORA widens the scope of outsourcing requirements on a wider circle of ICT TPPs. Important when considering the scope that DORA is not limited to the purpose of outsourcing whereas this guide is.	Reduce complexity, apply proportionality	Nordea Abp	Don't publish
2	1. Introduction 1.1. Purpose		1	Amendment	The definitions, especially the ones also defined in DORA, such as critical or important functions and ICT assets, should be aligned in this guide and with DORA, this is currently not the case	Ensure alignment	Nordea Abp	Don't publish
3	1. Introduction 1.1. Purpose		1	Amendment	The term "outsourcing" should only be used when referring to services that fall under the definition in the EBA Guidelines on Outsourcing. Not in general when referring to services that are being provided by 3rd party. Cloud services are not always outsourcing according to that definition.	Ensure alignment	Nordea Abp	Don't publish

4	1. Introduction 1.1. Purpose		1	Clarification	Please review the applicability of the passage "with many CSPs relying on proprietary technologies" as it mostly applies to Cloud services higher in the stack such as PaaS and SaaS. For IaaS the differences in technologies used by different CSPs applies to much lesser degree and this should be taken into consideration.	Consider deleting or clarifying the distinction further	Nordea Abp	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		6	Amendment	The guide contains several references to the NIS2 Directive, even though it has been confirmed that DORA is lex specialis to NIS2. Hence, there are a number of references in the Guide which can lead to misnterpretation. Consider removing references to NIS2.	Ensure alignment as financial entities are subject to DORA	Nordea Abp	Publish
6	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks		8	Amendment	DORA requirements which already raises a number of new parameters for tracking concentration risk (Recitals 66, 67, including the definition of ICT concentration risk in Article 3, 29 which is missing in the Guide, article 28 and 29 of DORA main regulation and Recital 6 of the ITS of the Register of Information, there are also references to concentration risk in several other RTS:s). Additionally, a risk assessment is already carried out for the purpose of contracting ICT services by the TPPs and another one when the TPP shoud consider changing a subcontractor which supports critical or important functions. Hence, separate risk assessment done only for CSPs, would make the assessment processes more complicated and add burden to the banks' risk management Practises. We propose to amend the section and refer to banks applying a risk-based approach and DORA.	Alignment to DORA requirements on concentration risk	Nordea Abp	Publish
7	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		11	Deletion	Propose to exclude "maintain an up-to-date inventory of all the ICT assets" as the consumer doesn't have possibility to retrieve the relevant CSP asset inventory	Information on ICT assets are not available	Nordea Abp	Publish
8	2.4 Exit strategy and termination rights 2.4.1 Termination rights		13	Deletion	Estimated cost for Exit strategies is a new requirement and not part of DORA as referenced, as this is a new requirement which adds further administrative burden, this should be analysed from cost and benefit perspective before adding a new layer on top of DORA requirements or exit strategies and plans and their testing.	Better alignment	Nordea Abp	Publish

9	2.4 Exit strategy and termination rights 2.4.2 Components of the exit strategy and alignment with the exit plan		13	Deletion	We strongly recommend to remove paragraph 2 as it appears to add new 3rd party risk management requirements specific to Cloud in addtion to those defined in DORA in the main regulation and articles 28-30. These additional requirements are already covered in the general requirements for all 3rd parties and further specification would add disproportional complexity for only one type of outsourcing.	Requirements are already covered	Nordea Abp	Publish