EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
Dutch Banking Association

Contact person

Mr/Ms
Mr

First name
Laurens

Surname
Messing

Email address
messing@nvb.nl

Telephone number
31612763904

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

General comments

The Dutch Banking Association on behalf of its members welcomes the opportunity to share views on the ECB's Guide on outsourcing cloud services to cloud service providers. Based on our key messages on this ECB Guide, the following highlights reflect the current understanding of our Dutch member banks. Our detailed comments can be found in the designated worksheet.

Definitions - The Guidance is using the BRRD definition of Critical and Important Functions, rather than the DORA definition which is unhelpful misalignment. Similarly, the definition of ICT asset should be that which is used in DORA. These are different definition than DORA. How should this 'non-binding' definition be applied in light of the binding definition of DORA?

Proportionate, risk-based interpretation of DORA – Many of the non-binding ECB expectation takes away nearly all possibilities to allow for a proportionate, risk-based interpretation of DORA.

Dual/Multi-provider requirement - Back-ups of critical functions are an important element of a financial entity business continuity plans, as noted by DORA. However, sub-subsection 2.2.1 of the Guide mandates financial entities to employ multi-provider requirement for critical or important functions. This is not in line with DORA and would potentially lead to increased risks and costs. This assumes that some major banks need to have two clouds available (could also be a major bank's data centre as fallback). Are we talking about other providers or is it possible to maintain a separate cloud environment with same provider? It implies that for critical functions we cannot use CSP specific solutions as this will limit the option to move this to another CSP or back on-premises. This would undermine many of the benefits of cloud services.

Backup strategy - The suggestion that back-ups of Crtical and Important Functions should not be stored in the cloud which hosts the services will not always be practically possible. For the organization, it can be very difficult to separate hosting and service backups because the cloud provider might use a specific database that cannot be backed up with another cloud provider or on-premises infrastructure. In our understanding of DORA 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.

Scalability - 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.

Contracting - While the guidance notes that DORA requirements remain the legally binding obligations, certain provisions within the guidance require further contractual remediation. The explicit suggestion in the guide that contracts with CSPs should be remediated as part of the ECB guidance should be deleted. The non-binding nature of the guidance means that CSPs are likely to push back on additional contractual remediation and the Guidance should recognise these practical difficulties. The new requirements in the ECB Guide are not addressed in the current DORA repapering of contracts and would mean a new re-papering of all contracts in 2025.

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	Chapter 1	1.1	1	Clarification	To start with, we need clarity on the legal status and binding nature of the supervisory expectations. On one hand, the Guide does not provide additional rules, but on the other hand, it appears that rules are indeed being imposed. Furthermore, the basis for most of the mentioned rules is not specified, and they seem to be in addition to the existing rules of DORA, NIS2, CDD, and EBA. The definition of “cloud service” lacks clarity. Institutions seek explicit guidance on which cloud services are not considered outsourcing. The concern is that widely available and not customized cloud services are not available for negotiation due to their standardized terms. We need clarification that using such cloud services do not constitute outsourcing when they won’t significantly impact critical processes. Since 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. Could you please confirm this. Last point that needs to be clarified: Article 21 of NIS 2 also includes some proportional approaches. Could you explain how these principles/approaches in NIS 2 and DORA interrelate and how entities can use them without risking conflicting interpretations.	We need clarification on the following topics: 1) On the legal status and binding nature of the supervisory expectations. 2) Definition 'Cloud Service' 3) Confirmation implementation ECB Guide according to the proportionality in DORA 4) Clarify that proportional approaches NIS2 and DORA interrelate	Messing, Laurens	Publish

2	Chapter 1	1.1	1	Clarification	Article 74 of the Capital Requirements Directive (CRD)3 deals with internal governance and recovery and resolution plans. It outlines robust governance arrangements for institutions. Article 74 also touches on accounting standards and remuneration practices. While it doesn't directly combine with DORA-Article 5, both are essential for financial stability and risk management. Our recommondation is to combine Article 74 with Article 5 of DORA.	Combine Article 5 of DORA wit Article 74 of the Capital Requirements Directive 3.	Messing, Laurens	Publish
3	Chapter 1	1.1	2	Clarification	We would request further clarification on the expectations. The guidance is stated to be non-binding, and secondary to the legally binding obligations of DORA. The language throughout shifts from practices which "should" be undertaken, to suggested best practice. If the ECB expects strict adherence to all aspects of the guidance, rather than allowing firms to take a risk-based, proportionate approach, this requirement should be explicitly stated.	We would request further clarification on the expectations. Expect ECB strict adherence to all aspects, rather than to take a risk-based approach.	Messing, Laurens	Publish
4	Chapter 1	1.1	2	Clarification	We need more guidance and clearity on the definitions EBA outcourcing rules. Because the definitions in EBA outsourcing rules differ and are not similar to the DORA, NIS2 definitions. To start with, there is unclarity about the definition of outsourcing.	We need more guidance and clearity on the definition outcourcing.	Messing, Laurens	Publish
5	Chapter 1	1.1	2	Amendment	BRRD (Bank Recovery and Resolution Directive) defines 'critical or important functions' different then the definition from EBA outsourcing and DORA. We recommend to alter definition or include expand name.	We suggest to align the definition of 'critical important function' with DORA.	Messing, Laurens	Publish
6	Chapter 1	1.1	2	Amendment	We strongly advise to remove existig definitions and refer to applicable guidelines. For example, align definitions as 'service provider' with the definition of 'third party service provider' under DORA. Another example it is unclear what is meant by CPS in case of SaaS, do you mean the SaaS provider or the underlying cloud platform provider.	We strongly advise to remove existig definitions and refer to applicable guidelines.	Messing, Laurens	Publish
7	Chapter 1	1.2	2	Clarification	We would request confirmation regarding the Guide is only applicability to Banks included in the list of supervised entities, as published on the SSM website.	We request confirmation the Guide is only applicability to Banks included in the list of supervised entities.	Messing, Laurens	Publish
8	Chapter 1	1.2	2	Clarification	We would like to point out that 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 those commonly used (e.g., from NIST). To avoid misinterpretation in definitions, we suggest substituting it with 'business,' 'enterprise,' or 'institution.'"	To avoid misinterpretation in definitions, aim to be consistent.	Messing, Laurens	Publish
9	Chapter 1	1.2	3	Clarification	The Guidance notes that DORA requirements are legally binding obligations. However, specific provisions within the guidance may necessitate additional contractual adjustments. Given the urgency for financial entities to meet DORA requirements by January 2025, we asking confirmation that there is no expectation of further remedations.	Given the urgency to meet DORA requirements by January 2025, we asking confirmation that there is no expectation of further remedations in contracts.	Messing, Laurens	Publish

10	Chapter 1	1.2	3	Clarification	We require clarity that the guidance, as the ECB's view on DORA, does not come into effect until the application of DORA from 17th Jan 2025.	Clarity that the Guide does not come into effect until the application of DORA.	Messing, Laurens	Publish
11	Chapter 1	1.2	3	Clarification	Further clarification is required regarding which party bears the obligation, whether it is the CPS or the financial enitity. For example the proposed approach on joint testing is unlikely to work in practice unless CPS is target of certain provisions.	Clarification is required regarding which party bears the obligation, the CPS or the financial enitity.	Messing, Laurens	Publish
12	Chapter 1	1.2	3	Deletion	We would prefer clarification on whether the ECB Guide is intended to indicate that it should be read alongside DORA and the EBA Guidelines on outsourcing arrangements. Unclear is it meant to convey that DORA takes precedence over both the ECB guide and the EBA guidelines on outsourcing arrangements. Our recommendation is to consolidate the ECB Guide within DORA instead of keeping them separate.	ECB Guide should be read alongside DORA. Our recommendation is to consolidate the ECB Guide within DORA instead of keeping them separate.	Messing, Laurens	Publish
13	Chapter 1	1.2	3	Clarification	ECB states that the Guide neither provides additional rules nor replaces existing ones. However, many paragraphs mention rules/guidelines that refer to "good practice". We require more clarity on what constitutes "good practice".	We require more clarity on what constitutes "good practice".	Messing, Laurens	Publish
14	Chapter 1	1.2	3	Deletion	The Guide states that the existing EBA guidelines continue to apply. The overlapping regulatory requirements create conflicting expectations, prevent scattered details across different guidances. For example, whether the provisions should apply to CIFs or to all services. The ECB should bear in mind that the ESAs want to address duplication between the DORA and the EBA guidelines, and therefore take a similar approach by stating that these guidelines take precedence.	The overlapping regulatory requirements create conflicting expectations, prevent scattered details across different guidances.	Messing, Laurens	Publish
15	Chapter 1	1.2	3	Amendment	We strongly recommend aligning the definitions with DORA. The Guide currently uses the BRRD definition of Critical and Important Functions, which misaligns with DORA. Another example is the definition of ICT assets, which differs from the DORA definition. Last example 'outsourcing' is not clearly defined in regulation and more confusion for supervised institusions will be caused if there is no common terminology in relation to outsoucing	Amendment suggestion, we strongly recommend aligning the definitions with DORA. Definitions as: Critical and Important functions, ICT assets and Outsourcing.	Messing, Laurens	Publish
16	Chapter 1	1.2	3	Clarification	We strongly recommend to provide more consistency regarding the types of cloud services within the scope. For example, whether this relates to cloud services supporting CIFs or all services, and which types of cloud service (IaaS/SaaS/ PaaS) are subject to specific requirements. If SaaS falls within the scope, it remains unclear whether it is expected to have full visibility of each cloud region topology supporting the SaaS. Without clarity the Guide will be lacking in proprotionality and enforceability.	We strongly recommend to provide more consistency regarding the types of cloud services within the scope.	Messing, Laurens	Publish

17	Chapter 1	1.2	3	Clarification	It is unclear to what extent the requirements should apply down the supply chain. We recommend limiting them to direct cloud services with which the financial entity has a contractual relationship. Without this limitation, there would be a lack of proportionality. For example, the sentence: 'Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply' should be limited in scope in order to be only addressed to CIFs.	Clarification is required regarding how far down the supply chain the requirements should apply.	Messing, Laurens	Publish
18	Chapter 2	2,1.1	4	Clarification	We would like to get the confirmation that the assumption is correct that the word use 'should' and 'ensure' imply that there is not strict obligation to comply, but merely imply a non-binding suggestion. Please clarify the binding status of the various requirements as laid down in the Guide; on the one hand, it is stated that the Guide "does not establish legally binding requirements", but on the other hand, it appears on several occasions that financial institutions are obliged to comply with the requirements by using the words "institutions should", see, for example, 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 also the use of the word "ensure" in the last bullet in 2.2.2	We request confirmation that the assumption is accurate: the use of the words ‘should’ and ‘ensure’ implies a suggestion rather than a strict obligation to comply.	Messing, Laurens	Publish
19	Chapter 2	2.1.1	4	Clarification	We need clarification on the scope. The first sentence of 2.1.1 already sets forth that the institution must have a clear governance framework. This sentence implies the governance framework is only needed to protect information. which seems to narrow. Also, the management body's responsibility is not limited to management of ICT risk, but remains responsible for outsourced activities under EBA outsourcing guidelines. We suggest the following amendment: replace the last to sentences of this paragraph by: "Nevertheless, the outsourcing contract must set out a clear and unambiguous allocation of roles and responsibilities."	We need clarification on the scope of the governance framework.	Messing, Laurens	Publish

20	Chapter 2	2.1.1	4	Amendment	The guidelines state: "The ECB understands Article 28(1)(a) of DORA as meaning that institutions which outsource ICT should apply the same level of diligence regarding risk management, processes, and controls (including ICT security) as those which decide to keep the relevant services in-house. Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls". Please replace 'equivalent' by 'appropriate'. Most customers will outsource part of the services and keep part on premise. The term equivalent seems to imply that the service provider must apply the same risk management processes and controls as the institution. The service providers will work for a range of customers and they are unlikely to adjust their risk management processes and controls for each individual customer. The customer must verify whether the risk management processes and controls are appropriate, taking into account proportionality.	Strong reccomondation to replace the word 'equivalent' (risk management). Our suggestion is to use the word 'appropriate' (risk management) instead.	Messing, Laurens	Publish
21	Chapter 2	2.1.2	4	Deletion	We advise to delete in the paragraph the governance responsibility. It is not new and already part of existing and applicable EU regulatory (DORA, EBA).	Remove the governance responsiility in this paragraph.	Messing, Laurens	Publish
22	Chapter 2	2.1.2	4	Clarification	Our recommendation is to rewrite the whole paragraph because of lack of feasibility and to ensure a more realistic approach. The current requirements exceed what can reasonably be contractually imposed on suppliers. Furthermore, the actual requirements are so high level that it is hard to understand the actual requirements. The only way that a financial entity can enforce any of these suggested requirements is via a contract, yet this provison is aimed at the pre-contractual phase. As an alternative framing, consider: "assess that the CSP has properly implemented relevant checks".	Our recommendation is to rewrite the whole paragraph because of lack of feasibility and to ensure a more realistic approach.	Messing, Laurens	Publish
23	Chapter 2	2.1.2	4	Clarification	We don't reconize the challenge of identifying an alternative provider. The real difficulty lies in the time and effort needed to migrate to an alternative provider. We recommend reconsidering the following text: "vendor lock - in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required".	We don't reconize the challenge of identifying an alternative provider. We recommend reconsidering the text about vendor lock.	Messing, Laurens	Publish
24	Chapter 2	2.1.2	4	Clarification	Could you please clarify whether localisation risk is included within the category of Data Storage and Processing risks.	Clarification is needed wheter localisation risk is included.	Messing, Laurens	Publish

25	Chapter 2	2.1.2	4	Amendment	Three risk scenarios/sentences may trigger an exit strategy. Both risks can be mitigated by switching providers, which aligns with the bullet point (vendor lock-in risk). Consider removing the following elements because of a lack of feasibility: 1) "the risk of a considerable fall in in quality or a significant increase in price' The risk of significant price increases often occurs in consolidating markets, where buyers raise prices after takeovers to recoup costs upon contract renewal. 2) The risk of considerable fall in quality is hard to predict. 3) Physical risks and region-specific risks. We expect physical risk to be region-specific.	We recommend to remove the risk scenario's about significant price increase, the risk of quality and phisical risks.	Messing, Laurens	Publish
26	Chapter 2	2.1.2	4	Clarification	Regarding multi-tenant environments, it is unclear what additional risks are considered beyond unauthorized data access.	It is unclear what additional risks are regarding multi-tenant environments.	Messing, Laurens	Publish
27	Chapter 2	2.1.2	5	Clarification	Although DORA refers to clause 28(4), the listed actions for financial entities to perform, partly based on 'good practice', but is is not clear where those actions originate from exactly.	Clarification is required on what the requested list of actions are based.	Messing, Laurens	Publish
28	Chapter 2	2.1.2	5	Clarification	We need more guidance how we can verify the following: "Assess whether the institution has the expertise and human resources required to implement and perform these checks".	More guidance is needed how verify expertise and human resources.	Messing, Laurens	Publish
29	Chapter 2	2.1.3	5	Clarification	The guidance does not make a differentiation between CSPs classified as 'critical' or not critical under DORA.	Potential inconsistency with DORA.	Messing, Laurens	Publish
30	Chapter 2	2.1.3	5	Clarification	The guidance extends beyond DORA obligations, with a broadening focus on ICT third-party risk management. In the ECB Guide, there's a requirement for a strategy that encompasses not only risks but also business elements and an operating service model. It's crucial to clarify that the concept of an outsourcing strategy should remain limited to risk management, as stated in DORA.	It's important to clarify that the concept of an outsourcing strategy should remain limited to risk management, as stated in DORA.	Messing, Laurens	Publish
31	Chapter 2	2.2.1	6	Amendment	The content is unclear because the requirements in the paragraph do not match 2.2.2. Does the whole section refer only to critical and important functions? There is ambiguity about the scope of all outsourced Cloud services. Does it address the entire chain including CoIF or not. Does '"in the cloud hosting the services" mean at the CSP level or some other separation level. Unclear it is then not suffice if you apply only CSP approach.	More clarification needed in this paragraph.	Messing, Laurens	Publish

32	Chapter 2	2.2.1	6	Clarification	To avoid compromising the security of network and information systems, the ECB considers that backups of critical or important systems should not be stored in the cloud hosting the relevant services. It is unclear whether this can be applied when the backup is located in another region. It is also unclear whether it is acceptable for the backup to be immutable at another CSP. Can you clarify whether you want all banks to maintain separate Solid State Drivers (SSDs) and/or Tape Robot to back up all Cloud data. We need more guidance what this mean in practice, for example with SaaS solutions primary servers handle live data and backup servers are designed to create and store copies of data from primary servers.	Clarification is requested about the back-up location. We need more guidance on how it works in practice.	Messing, Laurens	Publish
33	Chapter 2	2.2.1	6	Clarification	Can you advise us what is meant with 'cloud services', does it mean Iaas, Paas, Saas.	Please clarify what is meant with 'cloud services'.	Messing, Laurens	Publish
34	Chapter 2	2.2.1	6	Deletion	The requirement that back-ups of CIFs should not be stored in the cloud, goes beyond the EBA/DORA existing requirements and suggests a disconnect from technical reality. Recent experiences (for example with Unisuper) has demonstrated that back-up from within the same cloud service is at times criticial for recovery. Organizations may struggle to segregate hosting and service backups due to specific databases used by the cloud provider. In our understanding the backups could reside on a different network architecture (physically and logically segregated from the source ICT system), even if it belongs to the same CSP, and not necessarily be implemented on a completely different CSP. Please note that the measure to have back-ups stored in other cloud providers seems to be not applicable for SaaS Cloud and in any case would imply a huge effort with direct impact on the cloud benefits. In addition, it should be noted that the CSP ensures the BC through redundancy not through a backup system and that the article 12 of DORA refers in general to TPP (not specific to CSP).	The requirement that back-ups of CIFs should not be stored in the cloud, goes beyond the EBA/DORA existing requirements. This requirement is not realistic.	Messing, Laurens	Publish
35	Chapter 2	2.2.1	6	Deletion	The proposed worst-case scenario of an entire CSP being unavailable and uncooperative is not plausible. The only way to mitigate this would be to develop, maintain and scale several parallel systems performing the same functions with different architectures and infrastructure, which would mean doubling the cost and maintenance effort.	The proposed worst-case scenario of an entire CSP being unavailable and uncooperative is not plausible.	Messing, Laurens	Publish

36	Chapter 2	2.2.1	6	Deletion	We suggest deleting the following phrase because it is overly limiting, especially when it comes to the use of SaaS Solutions: "The institution must maintain the ability to bring data and applications back on-premises" or alternatively rewording it in line with the regulatory provisions as follows: "The institution must maintain the ability to bring data and applications back on-premises or transfer them to alternative CSPs or back-up providers". It should 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. Please clarify that backups can be stored with the same service provider, as long as the provider has redundancy in place to ensure that backup data or critical systems are not stored in the same cloud.	We suggest deleting the following phrase because it is overly limiting, especially when it comes to the use of SaaS Solutions. Please can you clarify that backups can be stored with the same service provider.	Messing, Laurens	Publish
37	Chapter 2	2.2.1	6	Clarification	The guidelines emphasize that Business Continuity Management (BCM) measures should address a worst-case scenario. Specifically, in this scenario, relevant cloud services provided by one or more CSPs are unavailable, and the institution must perform an exit under stress or without cooperation from the CSP(s). However, setting realistic Recovery Time Objectives (RTOs) for worst-case scenarios remains challenging, especially when migrating services to another cloud provider without assistance. The complexity and risks of synchronizing operations across multiple providers add further complications. DORA 12 (6) relates to RTO and RPO.	Setting realistic Recovery Time Objectives (RTOs) for worst-case scenarios remains challenging. We require more specific criteria to make it more measurable.	Messing, Laurens	Publish
38	Chapter 2	2.2.2	6	Amendment	These requirements seem to be more realistic thant the requirements in 2.2.1. But the titel states 'Critical functions', can you confirm this is the same as 'critical or important'.	The titel states 'Critical functions', can you confirm this is the same as 'critical or important'.	Messing, Laurens	Publish
39	Chapter 2	2.2.2	6	Amendment	The measures mentioned to contribute to resilience, which can be taken by the institution, are outlined here. However, one might interpret these measures (particularly bullet points 1 and 2) as actions applicable to the vendor. In that case, the institution’s responsibility lies in managing contractual requirements.	Confirm please that we interpret these measures correctly (particularly bullet points 1 and 2) as actions applicable to the vendor.	Messing, Laurens	Publish
40	Chapter 2	2.2.2	7	Amendment	This paragraph is lacking in proportionality. It should be amended to take account of the fact that maintaining multiple CSPs would be prohibitively expensive. Focus instead on mutliple back up providers.	This paragraph is lacking in proportionality.	Messing, Laurens	Publish

41	Chapter 2	2.2.2	7	Deletion	The level of prescription below 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. 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". We also recommend deleting: "The institution must retain the ability to bring data and applications back on-premises". Because this sentence has different requirements than previous part of the chapter	The level of prescription will ensure that the guidance quickly becomes out-of-date. We recommend deleting some parts of the text.	Messing, Laurens	Publish
42	Chapter 2	2.2.2	6	Clarification	The guidance will lead to variations in interpretation through the use of "may include". Would want confirmation that adapting these provisions on a proportionate basis will not conflict with ECB expectations.	Potential lack of confidence because unclearity about the worduse 'may include'.	Messing, Laurens	Publish
43	Chapter 2	2.2.2	6	Clarification	Regarding the reference to Article 6(8) of DORA, it should be viewed as a general provision that encompasses all technologies, including the Cloud. If we need to develop ad-hoc strategies for each project, it could weaken its implementation.	Ad-hoc strategies can weaken the implementation.	Messing, Laurens	Publish
44	Chapter 2	2.2.2	7	Clarification	We miss alignmend with the Data Act in the folowwing part of the Guide:"To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact of using a solution specific to an individual CSP. For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment." The Data Act contains obligations for CSPs to ensure the portability of data and systems. These obligations for institutions are therefore also dependent on the enforcement of the Data Act on CSPs	We recommend to align with the Data Act.	Messing, Laurens	Publish
45	Chapter 2	2.2.2	7	Clarification	The institution must retain the ability to bring data and applications back on-premises.To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimizing the impact of relying on a solution specific to an individual CSP. However, in the majority of cases, achieving this practicality is not feasible.	The institution must retain the ability to bring data and applications back on-premises.	Messing, Laurens	Publish

46	Chapter 2	2.2.2	7	Clarification	We need clarification on how to interpret the following scenario: According to Article 28(8) of DORA, the ECB expects institutions to ensure that abrupt discontinuation of a CSP's outsourced cloud services for critical functions does not result in business disruption beyond the maximum tolerable downtime or data loss defined in the institution's internal policies.	We need clarification on how to interpret that ensure that abrupt discontinuation of a CSP's outsourced cloud services for critical functions does not result in business disruption.	Messing, Laurens	Publish
47	Chapter 2	2.2.3	7	Clarification	To avoid misinterpretation and ambiguity, clarification is needed regarding whether the Disaster Recovery Plan (DRP) is related to CSP infrastructure or the institution's configurable services running in the cloud environment.	To avoid misinterpretation and ambiguity, clarification is needed regarding whether the DPR.	Messing, Laurens	Publish
48	Chapter 2	2.2.3	7	Amendment	It is not proportionally realistic to do spot checks of all services as part of tests for disaster recovery. It should be applied through a materiality lens. Similarly, non-reliance on disaster recovery certifications should be limited to IaaS.	It is not proportionally realistic to do spot checks of all services.	Messing, Laurens	Publish
49	Chapter 2	2.2.3	8	Amendment	We recommend that the Guide actively encourage CSPs to participate in joint testing. Our suggestion is to add the following: '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'.	We recommend that the Guide actively encourage CSPs to participate in joint testing.	Messing, Laurens	Publish
50	Chapter 2	2.2.3	8	Deletion	The suggestion that contracts with CSPs should be remediated as part of the ECB guidance should be deleted. The non-binding nature of the guidance means that CSPs are likely to push back on additional contractual remediation, and the Guide should recognize these practical difficulties. These difficulties will be exacerbated when applied to non-CSP third-party providers (TPPs) reliant on cloud services provided by a CSP.	The suggestion that contracts with CSPs should be remediated as part of the ECB guidance should be deleted.	Messing, Laurens	Publish
51	Chapter 2	2.2.3	8	Clarification	We require further guidance on how to address testing when joint testing with the CSP is not possible.	We require further guidance on how to address testing CSP's.	Messing, Laurens	Publish
52	Chapter 2	2.2.4	8	Amendment	The definitions of 'concentration risk' and 'lock-in risk' lack clarity. It's challenging to pinpoint their scope, and we're left wondering whether market share constitutes a concentration risk, for instance. Additionally, concentration risks must be considered in the policy governing the use of ICT services that support critical or important functions, as outlined in Article 1 (h) of DORA. I would anticipate the Guide to include a reference specifically addressing concentration risk related to geographical data storage, as that represents an actual risk.	The definitions of 'concentration risk' and 'lock-in risk' need more clarification.	Messing, Laurens	Publish

53	Chapter 2	2.2.4	8	Clarification	The concentration assessment provisions, which we undertstand to be at the entity level, fail to take account of the assessments to be undertaken by authorities as part of the incoming Critical ICT Third Party Provider regime. These should be leveraged, rather than expecting assessments on a regular basis by the firm. The preliminary assessment of ICT concentration risk obligated by Article 29 DORA is the key. The guidance should be embedded in the wider regulatory landscape. There is also a lack of clarity over whether the concentration risk is internal or external, and a need to recognise that In fact, it has to be considered that minimizing concentration could incur in significant trade-offs in matters of system complexity, performance and cost.	There is a lack of clarity on the concentration assesment.	Messing, Laurens	Publish
54	Chapter 2	2.2.4	9	Clarification	Whilst it is referred to clause 28(4) DORA, various considerations on concentration are mentioned for the FE, partly based on 'good practice', but it is not clear where those considerations originate from exactly. We ask to elaborate the text.	We require clarification about the good ractice considerations.	Messing, Laurens	Publish
55	Chapter 2	2.3.1	9, 10	Deletion	The lifecycle approach to data encryption is already at risk of becoming out-of-date, and goes beyond the lifecycle stages referenced in DORA. And we fail to see how the following would strengthen data security in the cloud: "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." The guidance should enable firms to take their own risk-based approach, recognising that increasing the number of technologies also increases the number of interfaces which could be exposed. Furthermore at this moment detailed policies and procedures are in place governing the entire lifecycle of encrypted data (i.e. generation, storage, usage, revocation, expiry and renewal).	We recommend to delete the lifecycle approach to data encryption.	Messing, Laurens	Publish
56	Chapter 2	2.3	9	Clarification	In our opinion the statement that "Institutions that outsource to the cloud continue to own their data. For that reason, it is good practice for institutions to restrict the locations where CSPs can store their data and apply appropriate tracing mechanisms to monitor compliance with those restrictions, while also ensuring that data can be accessed when needed." , restricts the bank from using CSP services.	This limits the bank's use of CSPs	Messing, Laurens	Publish
57	Chapter 2	2.3	9	Amendment	"Institutions that outsource to the cloud continue to own their data". This is a legal discussion: ownership of data can be contractually taken care of, but local laws (such as insolvency) can impact such contractual ownership.	Delete statement	Messing, Laurens	Publish
58	Chapter 2	2.3	9	Clarification	We would like to have more clarity on what is meant with "are warranted" in this context.	Clarity required for "are warranted"	Messing, Laurens	Publish

59	Chapter 2	2.3	9	Amendment	Although several security measures are mentioned we suggest to make a reference to the internal governance framework with which the control on on-prem devops is managed. This provides the opportunity to focus on the specific cloud risks and measures.	We recommend to incorporate internal governance frameworks to manage on-prem DevOps control, allowing a focus on specific cloud risks and measures.	Messing, Laurens	Publish
60	Chapter 2	2.3.1	10	Deletion	To avoid misinterpretation and ambiguity we advice to delete the application of micro segmentation and multi-cloud technologies in this pragraph because it is in our opinion neither encryption related nor enhancing data security.	We recommend to delete application of micro segmentation and multi-cloud technology in this pragraph	Messing, Laurens	Publish
61	Chapter 2	2.3.1	10	Clarification	We ask for clarification on which risk is mitigated because data protection can be achieved and managed through different measures, e.g. IAM but also encryption in which the vendor has a major role and embeds a risk based approach.	Clarification required for which risk is mitigated	Messing, Laurens	Publish
62	Chapter 2	2.3.2	10	Amendment	The recommendation should be a list of unacceptable countries based on the firm's risk management practices, rather than a list of acceptable countries. If the aim is to ensure that FIs are aware of data processing and storage requirements across jurisdictions, the ECB should not prescribe the method (e.g. list of acceptable or unacceptable countries) by which an FI conducts this.	Delete the recommendation for a list of acceptable countries and introduce a risk based approach.	Messing, Laurens	Publish
63	Chapter 2	2.3.2	10	Clarification	The risk of litigation is not clear with regard to "Legal and political risks". Does it refer to the risk that contracts are not enforceable in a court of law because the rule of law does not provide for short term proceedings to obtain intermediate measures timely? We assume institutions should also take into account laws hindering transferring the data out of a country and data privacy related risks?	Clarification required for the risk of litigation.	Messing, Laurens	Publish
64	Chapter 2	2.3.3	10	Amendment	We recommend to add in this paragraph the Self Build Applications on platforms next to the classification of ICT assets outsourced to CSP's as these also need to be classified and registered.	Self Build Applications on platforms need to be classified and registered as well.	Messing, Laurens	Publish
65	Chapter 2	2.3.3	11	Clarification	We ask for clarification as to whether our takeaway is correct that the inventory of all ICT assets seems contrary to its Cloud-based scope.	The scope of the guidance is cloud services, so there should be no broader obligation on other types of ICT assets.	Messing, Laurens	Publish
66	Chapter 2	2.3.4.1	11	Deletion	The requirement for individual clauses should be deleted. This guidance should focus on what is substantively required, and refrain from prescribing the format, i.e. by saying "Financial entities should their practices address…" This approach is inconsistent with the existing EBA approach to date and is going beyond the DORA obligations in prescribing the form as well as substance. .	Delete the requirement for individual clauses.	Messing, Laurens	Publish
67	Chapter 2	2.3.4.2	12	Amendment	We recommend to delete or rephrase the requirement "if a CSP has access to any of the institution’s systems or data, this should be properly documented and monitored using appropriate monitoring tools (which should also be reviewed on a regular basis)", because in some cases it is not possible to review teh CSPs monitoring tools .	Delete or rephrase requirement related to access CSP to any of the institution's systems.	Messing, Laurens	Publish

68	Chapter 2	2.3.4.2	12	Clarification	Does the requirement for monitoring include that the subject institution is to monitor the usage of tooling that may be in place within the CSP to comply with legal requirements of the CSPs native country? Especially considering such requests may come with secrecy ("gag") orders and providing such monitoring insights to their customers may be not be allowed under their native countries' national laws. Would the ECB expect the CSPs not agreeing to this rule be grounds for exiting the cloud agreement?	We ask for clarification of how far this monitoring obligation extends.	Messing, Laurens	Publish
69	Chapter 2	2.4.1	13	Deletion	The requirement on obliging CSPs to assist with a transition is superfluous given the legal obligations set out in the Data Act. Similarly the Data Act stipulates 7 months for the transition, which is not reflected in the ECB guidance. The guidance should be embedded in the wider regulatory landscape.	We recommend to delete the obligation for CSP to assist with a transition end allign it with the Data Act.	Messing, Laurens	Publish
70	Chapter 2	2.4.1	12	Amendment	The value of the guidance is in supplementing the legal requirements, not proposing alternative criteria. Additionally there are other ways in which to tackle the underlying risks and provide comfort to regulators, without the need to resort to termination. For example additional safeguards on risk management, including through the incoming CTPP regime.The Guidance creates new additional termination rights which go beyond existing practice. Various reasons listed for termination from (i) to (ix) are not in accordance with Article 28(7) of DORA and EBA requirements. Also it is is not clear where those additional reasons originate from. The following reasons for termination should be deleted: "i) an excessive increase in expenses ii) relocation of business units or data centres iii) merger or sale iv) failure to succeessfully execute cloud provider test migrations at the agreed times. (vii) significant changes to the management of cybersecurity risk in the chain of sub-contractors" Seeking to create non-binding termination rights which do not reflect existing legal or market practice is lacking both proportionality and feasibility. Furthermore CSPs are unlikely to accept additional termination rights given the non-binding nature of the Guidance.	We strongly recommend to rephrase the paragraph about termination rights.	Messing, Laurens	Publish
71	Chapter 2	2.4.4	14	Amendment	The lack of proportionality in not limiting such expectations to only services supporting CIFs is stretching the feasibility of the guidance. As is the requirement that exit plans should be reviewed and tested regularly. This is especially the case with regards to strong authentication for all users, as opposed to focusing on accessing those systems deemed critical.	Introduce proportionality in exiting under stress.	Messing, Laurens	Publish

72	Chapter 2	2.4.4	14	Deletion	The reference to conflicting legislation is likely pointing to potential third country sanctions. The guidance should remain technical in nature, rather than incorporating political discussions best reserved for other policy vehicles.	Deal seperately with conflicting legislation in the field of third country sanctions.	Messing, Laurens	Publish
73	Chapter 2	2.4.4	14	Clarification	With regard to "In the exit strategies that are required under Article 28(8) of DORA, institutions should include a business continuity policy catering for such a situation in order to ensure that the institution is able to withstand that scenario and has access to the data required to operate the service in question.", we would like to know whether the enforcement of the interoperability requirements of the Data Act support this.	We seek clarification whether the exit strategies are alligned with the Data Act requirements.	Messing, Laurens	Publish
74	Chapter 2	2.5.1	15	Amendment	We strongly suggest To adopt our amendments to the texts in bold. (..:) the internal audit functions of the institutions as the **third line of the control model** should regularly review, following a risk based approach, the risks stemming from the use of a CSP's cloud services. **The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.** **The institutions fulfill these requirements if the internal audit carries out, on the basis of up-to-date information, an overall risk assessment of the ICT risks of the institution for the purpose of drawing up the appropriate internal audit work plan. Depending on the outcome of the overall risk assessment, the intensity and frequency of the audit assignments may differ between specific areas.** **This Internal Audit risk assessment process is independent of the one mentioned in Section 12.2, although it will be used to inform the Internal Audit Risk Assessment, which will also take into account, inter alia, the third party certifications.**	Our amendments contribute to clarify : i) the role of IA as the third line in the control model; ii) that it provides assurance following a risk-based approach; iii) IA performs a risk assessment, which is independet from the RA perfoms by the first/second line; iv) this risk assessment process allows us to assess the risks to which the entity is exposed and, based on the result of this assessment, to prioritise the Internal Audit Plan.	Messing, Laurens	Publish
75	Chapter 2	2.5.1	15	Amendment	The Guidance should state that institutions are encouraged to consider whether pooled auditing is adviseable on a risk-based approach. It should however not specify how a pooled audit works in practice, given the need for different approaches across member states. In light of separate guidance being produced on pooled auditing this guidance should refrain from overlap.	Introduce a reference to pooled auditing in this guidance.	Messing, Laurens	Publish
76	Chapter 2	2.5.1	15	Clarification	We suggest to introduce other (monitoring) tools which should be taken into account as the ECB states that monitoring tools provded by a CSP might not be sufficient.	We seek more clarity about ECB's expectations for monitoring.	Messing, Laurens	Publish

77	Chapter 2	2.5.1	15	Amendment	The wording currently refers to all ICT risk management requirements rather than those relating to cloud.	We recommend to limit the ICT risk requirements to those for the cloud	Messing, Laurens	Publish
78	Chapter 2	2.5	15	Amendment	With regard to " 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…..". It's the responsibility of the designated owner in cooperation with the 3-lines and not of the IA.	Rephrase the sentence to make clear who is responsible.	Messing, Laurens	Publish
79	Chapter 2	2.5.1	15	Amendment	We suggest to add the requirements for an "independent expert" as described in the title.	We seek more clarity what an independent expert should meet.	Messing, Laurens	Publish
80	Chapter 2	2.5.2	16	Deletion	These requirements are in accordance with the DORA legislation and existing EBA guidelines. A general statement in the beginning of the document can limit further details that are already known.	We recommend to delete paragraph 2.5.2 due to the overlap with DORA and EBA guidelines.	Messing, Laurens	Publish
81	Chapter 2	2.5.3	16	Deletion	We strongly recommend the call for SCCs is dropped given that there is a EU forum already reviewing this issue. and it has not yet produced any standardised clauses. Risk of an incoherent approach from EU institutions is then not inconceivable. A better approach would be to say that in the contractual arrangement the following bullet points should be considered, potentially via SCCs.	We recommend not to draft SCC at this given moment but to consider an other approach.	Messing, Laurens	Publish
82	Chapter 2	2.5.3	16	Deletion	The recommendation that "contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indicating the maximum cost" should be deleted. This goes beyond existing practice and is not in accordance with the EBA Guidelines. The Guidance should interpret the existing legal obligations rather than adding to them through new levels of practical prescription.	We recommend to delete the obligation to include details of how cost of performing on-site audits is calculated.	Messing, Laurens	Publish
83	Chapter 2	2.5.3	16	Amendment	The Guidance should state that institutions have taken safeguards against unilateral changes, rather than determining where a separate copy for digital provisions is required for these purposes. Setting out requirements for particular incidents will create partial coverage. The guidance should be outcomes focused.	Rephrase the obligations that institutions should take against unilateral changes.	Messing, Laurens	Publish
84	Chapter 2	2.5.3	16	Deletion	We recommend to delete the following sentence "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". as this will not be acceptable to most commonly used non-tailor-made services by CSPs. The requirement should be only related to those CSPs that are under the direct supervision due to DORA.	We strongly recommend to delete the obligation to sign a separate digital or physical copy.	Messing, Laurens	Publish