EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
Association of German Public Banks (VÖB)

Contact person

Mr/Ms
Ms

First name
Astrid

Surname
Freier

Email address
astrid.freier@voeb.de

Telephone number
0049308192184

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

General comments

Given that DORA and the supplementary ESA standards lay down extensive and stringent requirements for all entities in the financial sector, which also include cloud services and were developed with the involvement of supervisory authorities, IT and outsourcing experts among others, we appreciate the effort made by the ECB to put forward this Guide.

Going through the text, we would like to call for a **clear-cut alignment of this Guide with DORA**, in order to avoid misinterpretation and introducing additional requirements which do not exist in the DORA. We argue for **consistency and coherence between the DORA and the ECB Guide** in order to achieve a great level of clarity and simplicity.

With regards to DORA, we miss a clear statement that the expectations in the ECB guide can be implemented in a **risk-oriented** manner and by applying the standard of **proportionality**.

In addition, we strongly wish a harmonized **reflection with cloud and outsourcing** specific regulation. Some clauses can be read as introducing new and additional requirements. Overlapping regulatory requirements create conflicting expectations, in particular whether the provisions should apply to ciritical or important functions or all services, and do not convey the avoidance double regulation.

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 1.2 Scope and Effect		3	Amendment	"The ECB Guide refers exclusively to the portfolio of procured cloud solutions." We suppose that it cannot be the intention, for instance, the simple external procurement of goods supported on a secondary level by cloud (e.g. for delivery planning) or service providers (not directly supporting a critical function) that use off the shelf cloud applications (such as O365) should be associated with cloud service provision. We suggest either removing or reformulating the sentence "***Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply***."		Association of German Public Banks	Publish
2	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question		4	Amendment	"Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls."	It is not appropriate for third-parties to establish "*equivalent*" risk management practices to a financial entity. Risk management and contractual frameworks between FEs and third-parties impose appropriate risk management obligations on third-parties. We therefore suggest the following amendment: Consequently, institutions should ensure that their CSPs have established equivalently effective risk management practices, processes and controls.	Association of German Public Banks	Publish

3	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		5	Clarification	Under Art. 28 (4) DORA, instititutions are required to conduct risk analysis...prior to entering into a new outsourcing arrangement with a CSP. In order to adequately identify . the institutions should: We suggest to replace “institutions should” by “best practice shows...”	Within the framework of the requirements care must be taken to ensure that the institutions do not always conclude contracts with service providers who have already implemented such controls. Normally, service providers set up such controls once they want to work with us. In these cases, the institutions cannot check whether the controls are functional and suitable as part of the pre-outsourcing audit. Therefore, an audit of the controls before outsourcing should not end up on the mandatory agenda of the auditors, and only be considered “best practice”.	Association of German Public Banks	Publish
4	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		5	Amendment	Art. 2.1.2. mentions „vendor lock-in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required“ as good practice to consider risk. We suggest to add “if required and possible” given the strong contractual ties.		Association of German Public Banks	Publish
5	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	6	5	Deletion	The consideration of "**physical risks and region-specific risks (e.g. political stability risks)" and "the risk of a considerable fall in in quality or a significant increase in price (both of which are common scenarios in a highly concentrated market)" go beyond the existing EBA requirements or DORA**. Additionally, the risk of a considerable fall in quality is highly subjective and should be deleted. Both references should be deleted	Lack of **feasibility and proportionality**. The Guidance is building on existing requirements, rather than providing an interpretation.	Association of German Public Banks	Publish

6	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	3	6	Deletion	It indicates that institutions must have the **capacity to bring the data and backups on-premises**. 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. We therefore suggest deleting the phrase "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"	Having **on-premises backups is not always technically feasible**. In addition, tailored-business continuity plans to the specific risks and capacities of the institution, focusing on practical and achievable measures would provide equivalent solution.	Association of German Public Banks	Publish
7	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		6	Deletion/Amendment	The interpretations regarding the ability to bring data back on-premises and regarding portability go far beyond the DORA and should therefore be deleted or formulated to "***may*** ". Separate storage locations for backups can be costly and operationally challenging, particularly for smaller institutions.	Smaller banks may not have data centers or on-prem is very expensive, it would make more sense to refer to another technical area (no on-prem) or rather use a risk-based approach based on the bank's own risk assessment as a recommendation	Association of German Public Banks	Publish
8	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	4	7	Amendment	Spot checks on all services as part of diaster recovery tests would not be possible. Should be applied through a materiality lens. Similarly, not relying on disaster recovery certifications should be limited to IaaS.	Lacking in **proportionality**	Association of German Public Banks	Publish

9	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks		8	Clarification	The Guide should expressly state that financial entities (FEs) concentration risk should be assessed on a risk-based approach. Additionally, the concentration risk indicators are overly expansive, incorporating numerous factors that lack sufficient relevance to an accurate assessment of concentration risk and imposing both an unrealistic and unmanageable burden on risk management practices. This accounts in particular for the assessment of the scalability of the cloud which allows it to be gradually extended to encompass new functions.	It is unreasonable to expect FEs to account for all these indicators. In particular, the expectation for firms to consider the extent to which other supervised firms are reliant on the same CSPs requires an assessment of sector-level concentration risks, which is beyond individual FEs capacity and responsibility to consider. We would suggest to delete the last sentence in 2.2.4 given that scalability cannot be checked in an abstract way if the underlying functions are not clear yet. Therefore, we propose an integrated approach to address the topic holistically, but avoid a lack of clarity by aspects which cannot be adhered to during the assessment.	Association of German Public Banks	Publish
10	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and cryptographic key management processes		9	Amendment	The level of "*best practice* " is inadequately high especially with regards to cryptographic keys. There are additional means of a similar level of security "Best practice" should be replaced by "examplary measures".	The overall encryption process creates an unnecessary amount of work. Some institutions do not use cryptography entirely, but different means like network segmentation to obtain the same level of security.	Association of German Public Banks	Publish
11	2.3 ICT, security, data confidentiality and integrity 2.3.2 Risks stemming from location		10	Deletion	„Furthermore, the ECB also considers it good practice for institutions to assess additional risks if a sub-contractor relevant for the cloud services is located in a different country from the CSP, while taking into account any risks associated with complex sub-outsourcing chains as outlined in paragraph 25 of the EBA Guidelines on outsourcing arrangements."	This is extremely demanding and for most of the time more than 100 subcontractors of a CSP not feasible in practice". In addition, so far from a data protection point of view the assessment obligation is only given for the sub-contractor in scope, and not holistically for the entire sub-contractor chain	Association of German Public Banks	Publish
12	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.3 Consistent inclusion of outsourcing assets in an institution's inventory of ICT assets		10	Clarification	"Classification of all ICT assets" in an up-to-date inventory does not reflect enough the criticality and creates an inappropriate burden. We suggest to include a risk-based approach.	The inclusion of all ICT assets is an immense burden for the reporting entities and does not reflect the rationale behind DORA of identifying the CCSPs. It should be done on a risk-based approach including proportionality.	Association of German Public Banks	Publish

13	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements		11	Amendment	It may be viable to compare this requirement to standard privileged access management procedures. It should be sufficient that the IAM policy is reflecting cloud outsourcing and is regularly reviewed in the outsourcing agreement	Given the complexity and frequent changes of IAM policies the reflection ot the exact content in the outsourcing agreement goes beyond the DORA framework. Therefore only the existence and regular review of the IAM policy should be stated.	Association of German Public Banks	Publish
14	2.4 Exit strategy and termination rights 2.4.1 Termination rights	4, 5	12	Deletion	The Gudiance creates new additional termination rights which go beyond existing practice. The following 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."	Seeking to **create non-binding termination rights** which do not reflect existing legal or market practice is lacking both proportionality and feasibility. This goes beyond DORA and EBA requirements.	Association of German Public Banks	Publish
15	2.4 Exit strategy and termination rights 2.4.1 Termination rights		12	Amendment	“2.4.1 (2) describes other changes that could also lead to such a reason for terminating for termination, including in particular (iv) relocation... and (vi) change in the regulations applicable... For iv)and iv) we suggest to add “unless the data is immediately transferred to a host country that also otherwise meets the requirements of the outsourcing agreement".	None of these points are within the CSP's sphere of influence. Such clauses must give the CSP an opportunity to perform the contract correctly. Therefore the institutions may not be able to enshrine a corresponding clause in the context of general terms and conditions in a legally effective manner unless at the same time a remedy for the CSP is agreed (e.g. by moving). In a case of doubt it should be sufficient that a service will then be provided by another CSP and not by the institution itself.	Association of German Public Banks	Publish
16	2.4 Exit strategy and termination rights 2.4.2 Components of the exit strategy and alignment with the exit plan		13	Deletion	These interpretations go far beyond DORA, we suggest to be aligned with DORA. Art. 28 (8) DORA: For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7.	Art. 28 (8) DORA does not outline a principle based exit strategy with granular technical exit plans for individual cloud outsourcing arrangements: The exit plan should follow the risk based approach as outlined the overall framework of DORA. It has to be realistic and feasible, based on plausible scenarios and reasonable assumptions incl. a timeline which corresponds to the exit and termination conditions:	Association of German Public Banks	Publish
17	2.5 Oversight, monitoring and internal audits		15	Clarification	“An institution’s internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts). ”	Audits of hyperscalers should be replaced by regular neutral and independent certification for the services concerned initiated by the hyperscaler and confirmed by the supervisory authorities.	Association of German Public Banks	Publish

18	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	3	15	Amendment	The Guidance should state that institutions are encouraged to consider whether pooled auditing is adviseable, on a risk-based approach. It should not specify how a pooled audit works in practice, given the need for variations in approach across member states.	In light of separate guidance being produced on pooled auditing this guidance should refrain from overlap.	Association of German Public Banks	Publish
19	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	4	15	Amendment	The wording currently refers to all ICT risk management requirements, rather than those relating to Cloud.	Extension of scope in the guidance beyond Cloud.	Association of German Public Banks	Publish
20	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs		15	Clarification	Given that the institutions and CSPs work closely together, we suggest limiting additional monitoring to cases, in which the institution has reason to believe manipulation has occurred.		Association of German Public Banks	Publish