EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
Google Cloud

Contact person

Mr/Ms
Mr

First name
Julian

Surname
Schmücker

Email address
jschmuecker@google.com

Telephone number
0032 474 981209

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

General comments

Google Cloud prioritizes operational resilience, offering innovative, secure services to financial institutions. Our advanced cloud technologies, including infrastructure redundancy, automatic failover, disaster recovery tools, and security features, enhance operational resilience. We prioritize compliance and security, undergoing regular audits and certifications.

Google Cloud is a trusted partner for organizations seeking operational resilience, offering a comprehensive suite of technologies, services, and resources for building and maintaining resilient cloud systems. Our comprehensive customer support, including documentation, best practices and training, helps customers achieve resilience.

Compliance with the regulatory framework of the European financial sector is a cornerstone of our service offer. Over the past years, we have developed a dedicated compliance posture with respect to European and national financial supervisors' guidance on cloud outsourcing. As of 17 January 2025, the Digital Operational Resilience Act (DORA) will apply as the essential framework for ICT service provision and consumption in the financial sector. Google Cloud welcomes DORA as a crucial step towards accelerating digital innovation in Europe.

DORA creates a solid framework to enhance understanding, transparency, and trust among ICT providers, financial entities, and consumers. This fosters an ecosystem of cooperation and resilience. We recognize the pivotal role of DORA in raising the bar for cybersecurity and operational resilience across the financial sector. In turn, we support the structured risk management approach of DORA, emphasizing the importance of identifying, assessing, and mitigating risks. We have been constructively supporting the EU institutions' and ESAs' work on DORA during the last years. Continued close collaboration with financial services customers remains important to meet the requirements of DORA effectively. We look forward to supporting our customers in the preparatory period during 2024, providing engagements, guidance material and thought leadership on scalable compliance such as the approach to pooled Threat-Led Penetration Testing.

We call on the ECB to position its guidance on outsourcing cloud services to cloud service providers in the context of DORA. In order to allow a consistent and efficient implementation of the final DORA requirements, it is fundamentally important to align supervisory expectations with the requirements of the upcoming DORA framework. While we appreciate the ECB's attention and dedication to securing operational resilience, we identified a number of aspects where the proposed consultation document deviates from DORA. We offer respective proposals for amendments, clarification and - in limited circumstances - deletion, to address this fragmentation.

Key issues include: The guidance on backup systems should prioritize successful outcomes over specific methodologies, and it shouldn't limit exit strategies to on-premises solutions when DORA allows alternative providers. Direct testing of a CSP's disaster recovery plans poses security risks, and it is not practical or necessary for institutions to agree individual clauses with the CSP on a configuration-by-configuration basis. Additionally, the proposed termination grounds and scenarios in Section 2.4.1 go beyond DORA's requirements and create conflict. Lastly, the subcontractor requirements in that section overlap with and create confusion regarding the RTS on Subcontracting.

We believe that an ECB guidance aligned with DORA will support the financial industry's continued adoption of innovative cloud services. This will advance efficiency and resilience to the benefit of financial entities and ultimately customers in Europe.

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 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 guidance on back-ups for critical or important systems should focus on outcomes and not dictate methodology and must be consistent with DORA. This text should be deleted: "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." Alternatively, the text should be amended as follows: In order to avoid jeopardising the security of network and information systems, the ECB considers that DATA back-ups of critical or important systems should [DELETE: not] be stored in PHYSICALLY AND LOGICALLY SEGREGATED SYSTEMS FROM THE SOURCE ICT SYSTEM [DELETE: the cloud which hosts the services concerned].	We recognise the importance of ensuring the continued availability of critical or important systems. However, we urge the ECB to focus its guidance on the desired outcome (the availability of back-ups) as opposed to prescribing the methodology for achieving that outcome (not storing back-ups on the same cloud as the primary system). Taking an outcomes based approach is more proportionate and will help to future-proof the guidance against technological advances. If the prescriptive expectation is retained, then as a minimum it must be aligned with Article 12(3) of DORA, which says "When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system." We believe the reference to "back-ups" already refers to data back-ups. However, without clarification it could be read to refer to system back-ups. An expectation that institutions back-up entire systems (i.e. architecture/deployments/applications) on a different cloud is disproportionate as it would require the institution to simultaneously run two separate cloud environments on an ongoing basis.		Publish
2	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Amendment	The guidance should not restrict exit strategies and plans to bringing data and applications back on-premises when Article 28(8) of DORA also permits transfers to alternative providers. The text should be amended as follows: The institution must retain the ability to bring data and applications back on-premises OR TRANSFER DATA AND APPLICATIONS TO AN ALTERNATIVE PROVIDER. To this end, institutions should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while considering CONSIDERING [DELETE: minimising] the impact of using a solution specific to an individual CSP. [DELETE: 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].	Article 28(8) of DORA does not limit exit strategies and plans to bringing data and applications back on-premises. Instead, Article 28(8) refers to both" transfer[ing] them to alternative providers or reincorporat[ing] them in-house". We do not believe that the ECB intends to exclude options explicitly permitted under DORA and recommend that this text is clarified. In addition, although Article 29(1)(a) of DORA requires financial entities to consider substitutability, DORA does not require financial entities to "minimise the impact of using a solution specific to an individual CSP". This expectation poses serious risks to both resilience and innovation as financial entities would be pushed to rely on technology that is the lowest common denominator of what is available from third parties or on-prem. For example: -This expectation may prevent an institution from using the most suitable technology that achieves the best outcomes for its stakeholders simply because they may not be able to replicate that functionality with a different provider or on-prem in an exit scenario. -This expectation may push institutions to develop environment agnostic deployments that are in fact less resilient and less effective from a day-to-day perspective just so they can achieve a smoother migration path away from the CSP in an exit scenario. We recognise that exit planning is important to resilience, but expecting financial institutions to prioritise exit over business-as-usual outcomes is disproportionate and does not enhance the resilience of the institution or the sector as a whole. Instead, the focus should be on a proportionate and risk-based approach to balancing business-as-usual and exit requirements. Finally, we urge the ECB to focus its guidance on the desired outcome (effect migration) as opposed to prescribing the methodology for achieving that outcome (virtual machine based application or containerisation). Taking an outcomes based approach is more proportionate and will help to future-proof the guidance against technological advances.	Schmücker, Julian	Publish

3	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy	2.2.3	7	Amendment	It is not safe for institutions to test a CSP's disaster recovery plans directly. The text should be amended as follows: On the basis of these provisions, the ECB understands that an institution should ASSESS [DELETE: test] its CSP's disaster recovery plans AND TESTS and should not rely exclusively on relevant disaster recovery certifications. When ASSESSING [DELETE: conducting] disaster recovery tests with the CSP, the institution should [DELETE: perform spot checks and/or tests at short notice in order to] assess its readiness for an actual disaster event. The CSP'S testing plan should cover a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures). These scenarios should be tested regularly in accordance with the institution's strategy and in line with its business continuity policy and requirements. Alternatively, the text should be amended as follows: On the basis of these provisions, the ECB understands that an institution should PARTICIPATE IN testS OF ITS its CSP's disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications. When PARTICIPATING IN [DELETE: conducting] disaster recovery tests with the CSP, the institution should [DELETE: perform spot checks and/or tests at short notice in order to] assess its readiness for an actual disaster event. The CSP'S testing plan should cover a variety of disaster recovery scenarios (including component failure, full site loss, loss of a region and partial failures). These scenarios should be tested regularly in accordance with the institution's strategy and in line with its business continuity policy and requirements.	Public cloud services are multi-tenant environments. In this context, disaster recovery (DR) testing must be conducted in a way that safeguards all the CSP's customers. This is only possible with careful planning and robust guardrails. An expectation that each institution directly and individually test the CSP's DR plans exposes all the CSP's customers to an undue operational risk (this includes other institutions and financial entities). This is especially the case if the expectation is for institutions to conduct tests at short notice. We recognise that it is important for institutions to understand a CSP's ability to withstand and recover from disruptions/disasters. However, we strongly recommend that institutions are encouraged to do this by assessing the CSP's DR plans, DR testing approach and DR testing results. This gives institutions more insight than reviewing certifications whilst protecting all customers from significant incremental operational risk. If the ECB proceeds with an expectation for institutions to test the CSP's DR plans, then we urge the ECB to clarify that this should be achieved by the institution observing or participating in testing performed by the CSP. This is the only way to ensure testing is subject to appropriate safeguards.	Schmücker, Julian	Publish
4	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	The reference to data residency in Section 2.2.4 is inconsistent with DORA. The text should be clarified as follows: When performing risk assessments, the ECB considers it good practice to scrutinise typical risks relating to cloud services (such as increased provider lock-in, less predictable costs, increased difficulty of auditing, concentration of provided functions and lack of transparency regarding the use of sub-providers), alongside aspects of data LOCATION [DELETE: residency].	We believe the reference to "data residency" in Section 2.2.4 refers to an expectation that the institution considers the location of the institution's data. However, given how the term is commonly used, the reference to "data residency" could be read as an expectation that institution's data be located in a specific location. This would be inconsistent with Recital 82 of DORA which says "This Regulation does not impose a data localisation obligation as it does not require data storage or processing to be undertaken in the Union." To avoid this confusion, we recommend using the term "data location".	Schmücker, Julian	Publish
5	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	The reference to "executing" IAM policies in Section 2.3.4 is unclear. The text should be clarified as follows: An institution's IAM policy should be extended to cover cloud assets and IMPLEMENTED [DELETE: executed] when entering into a cloud outsourcing arrangement. This policy should cover both technical and business users	We believe the reference to "executed" in Section 2.3.4 refers to an expectation that the institution's IAM policy should be implemented when entering into a cloud outsourcing arrangement. However, given how the term is commonly used, the reference to "executed" could be read as an expectation that institution and the CSP sign the institution's IAM policy or otherwise incorporate it in the contract. An institution's IAM policy is internal to the institution and for security reasons should not be shared with the CSP. Nor is it appropriate for an institution's IAM policy to be included in the contract with the CSP because it exclusively contains responsibilities for the institution that are entirely within the institution's control when using a cloud service.	Schmücker, Julian	Publish
6	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	2.3.4.1	11	Amendment	It is not practical or necessary for institutions to agree individual clauses with the CSP on a configuration-by-configuration basis. The text should be amended as follows: The ECB considers it good practice for institutions to CONSIDER [DELETE: agree] individual clauses with the CSP when ENTERING INTO A CLOUD OUTSOURCING ARRANGEMENT [DELETE: configuring the cloud environment].	Public cloud services are one-to-many, standardised services. They operate in the same way for every customer. We agree that it is important for institutions and CSPs to understand their different areas of responsibility and that should be addressed in the contract. We also recognise that institutions should be able to negotiate contracts with CSPs to ensure the institutions requirements are addressed. That said, negotiation should happen during the pre-deployment phase. It is not appropriate to expect institutions to include individual clauses in the contract with the CSP on a configuration-by-configuration basis. Firstly, cloud services are typically contracted for under a framework contract or master services agreement. This applies to all workloads/use cases that the institution chooses to configure and deploy and the institution can choose to deploy new workloads or reconfigure existing workloads at any time. In this context, it is not practical or appropriate to expect the institution to include individual clauses in their contract with the CSP each time they configure the cloud environment. Instead, the institution should focus on whether the contract and their use of the services aligns with their defined requirements during the pre-deployment phase. Secondly, configuration is a customer responsibility in the public cloud context. This is particularly the case for IaaS and PaaS. The CSP's obligations don't change based on how the customer chooses to configure their cloud environment. The CSP's obligation remains to ensure the features and functionality operate as described. As this obligation is universal (and not dependent on specific configuration), an expectation that institutions agree individual clauses with the CSP when configuring the cloud environment is redundant and confusing.	Schmücker, Julian	Publish

7	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Deletion	The additional grounds of termination and termination scenarios in Section 2.4.1 conflict with and exceed the DORA requirements. The first two paragraphs of Section 2.4.1 should be deleted.	Article 28(7) of DORA is clear about the circumstances in which financial entities should be able to terminate. The ECB's expectations regarding grounds of termination overlap with and in many cases go beyond the four requirements in Article 28(7). For example: -"ongoing inadequate performance" overlaps with and sets a lower and less precise threshold than Article 28(7)(a), (b) and (c) -"serious breaches of the contractual terms, or of the applicable law or regulations" completely overlaps completely with Article 28(7)(a) but uses different words -"an excessive increase in expenses under the contractual arrangements that are attributable to the CSP" does not clearly map to any part of Article 28(7). This will add significant confusion to contracting for cloud services without a clear foundation within or consistency with DORA. It also appears to single-out and prejudice cloud services despite similar considerations applying to all ICT services and outsourcing. The ECB's proposal to include a list of scenarios that could trigger a grounds of termination is also confusing. Termination rights should be based on whether the grounds of termination in Article 28(7) of DORA are in fact present. This is inherently a subjective analysis based on the relevant circumstances. It cannot be based on a standard list of events that may or may not in reality trigger grounds for termination.	Schmücker, Julian	Publish
8	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	13	Amendment	The subcontractor requirements in Section 2.4.1 overlap with and create confusion regarding the RTS on Subcontracting. The fifth paragraph of Section 2.4.1 should be deleted.. Alternatively, the text should be amended as follows: On the basis of the requirement concerning key contractual provisions contained in Article 30(2)(a) of DORA, institutions should ensure that WHERE RELEVANT all SUBCONTRACTORS THAT EFFECTIVELY UNDERPIN THE PROVISION OF THESE ICT SERVICES [DELETE: suppliers of subcontracted services supporting the CSP] comply with EQUIVALENT [DELETE: the same] contractual obligations that apply between the institution and the CSP, (including obligations relating to confidentiality, integrity, availability, the retention and destruction of data, configurations and back-ups) if termination rights are exercised.	The conditions under Article 30(2)(a) of DORA are the subject of regulatory technical standard to be prepared by the ESAs pursuant to Article 30(5). The ECB should not propose overlapping expectations before the final version of the RTS is available. In particular, we note that the ECB's consultation closes on 15 July 2024. This is two days before the DORA deadline for the ESAs to submit the RTS to the Commission. Given the circumstances, no stakeholders responding to the ECB's consultation will have been able to assess them against the final RTS. We are concerned that this does not provide a meaningful period of consultation. Beyond the procedural concerns, the ECB's proposal raises a number of substantive concerns in light of the draft RTS. Firstly, the ECB proposal uses the phrase "suppliers of subcontracted services supporting the CSP". This phrase is not used in DORA or the draft RTS. Therefore, it is not possible to clearly map it to definitions in the legislative acts, some of which are still to be determined in the RTS. Secondly, the draft RTS contains requirements about flowing down contract terms to subcontractors that overlap with this proposal (see Article 3 and 4 of the draft RTS). The ECB's proposal that subcontractors be subject to the "same contractual obligations" is more consistent with a traditional outsourcing service model and is not compatible with cloud services. It is feasible in a traditional outsourcing service model for the primary contract to be replicated in the subcontract or for the primary contract to dictate details of the subcontract. This is because, in the traditional context: -the primary provider typically transfers an entire ICT service (all the services under the primary contract) or a discrete part of the service (all the services in one or more delivery schedules of the primary contract) to the subcontractor. -the service is one-to-one (i.e. subcontractors are engaged to support specific customers on an individual basis). So there's only one set of primary contract terms that need to be passed-through to subcontractors. This is not how subcontracting works in the public cloud service model: -The CSP may subcontract components of the service (e.g. technical support). These components are building blocks of the overall service, but they don't always have a one-to-one relationship with the service provided by the CSP. Therefore, it is not possible to simply replicate terms in the primary contract in the subcontractor. Instead, the primary contract should set these expectations as between the financial entity and the provider and require the provider to ensure that they are addressed in the subcontract without dictating how. -the service is one-to-many. A single subcontractor engaged by a CSP is relevant to potentially all the CSP's customers. Although the CSP will have a separate contract with each financial entity (this could be hundreds of financial entities), it will only have one contract with the subcontractor. It is not possible for that contract to replicate the terms of all the individual financial entity contracts.	Schmücker, Julian	Publish
9	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	2.5.2	16	Clarification	Use of cloud services does not necessarily entail outsourcing of reporting obligations under Article 19(5) of DORA. The reference to Article 19(5) of DORA in Section 2.5.2 should be clarified to explain the relationship between Section 2.5.2 and Article 30(2)(f) of DORA.	It is not clear if and how the ECB's expectations in Section 2.5.2 are relevant to Article 19(5) of DORA. Article 19(5) refers to the scenario where a financial entity outsources its reporting obligations under DORA to a third party service provider. That does not happen simply because an institution uses a cloud service. Typically, when using a cloud service - although the CSP will need to provide relevant information about incidents that occur in the CSP's area of responsibility - the institution retains the responsibility for its reporting obligations (i.e. the institution reports incidents to the relevant authority, not the CSP). This relationship is already addressed in Article 30(2)(f) of DORA and it is unclear whether the ECB intends to build on this requirement (or on requirements specific to Article 19(5)). If the ECB intends to build on Article 30(2)(f), it is unclear what the basis of these further requirements is under the legislative texts.	Schmücker, Julian	Publish

10	Box 2: Contractual clauses	2.5.3	16	Deletion	The recommendation to use standard contractual clauses in Section 2.5.3 is premature as no such clauses yet exist. Section 2.5.3 should be deleted	The ECB's proposed recommendation that financial entities use standard contractual clauses seems premature when no such standard contractual clauses yet exist. Also, it is unclear how financial entities are meant to apply the four recommendations about specific clauses when it is the public authorities - and not the financial entities - that will define the content of the standard contractual clauses referenced in Article 30(4) of DORA. As a public authority, the ECB is well-positioned to contribute to any standard contractual clauses referred to in Article 30(4). Rather than directing best practices at financial entities, it would be more effective to direct them to the public authorities drafting those clauses. In this context, the only appropriate obligation or expectation on financial entities is one to consider relevant standard contractual clauses as-and-when they become available. We urge the ECB not to pre-empt this by positively recommending the use of as-yet undefined clauses. If the ECB's intent is to propose best practices for contracts other than those referenced in Article 30(4), then it is not clear how these expectations relate to (or avoid conflicting with) Articles 30(2) and (3), which clearly set out the requirements for contracts under DORA.	Schmücker, Julian	Publish