EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company

European Savings and Retail Banking Group

Contact person

Mr/Ms

Ms

First name

Janine

Surname

Barten

Email address

janine.barten@wsbi-esbg.org

Telephone number

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

General comments

In general, the European Savings and Retail Banking Group (ESBG) believes that the draft guidance does not take into account the proportionality included in DORA and reduces the level of resilience required in DORA, because it limits the possibilities of using the cloud, when the cloud enables both physical and logical separation.
We highlight the over-regulation of CSPs. CSPs have to comply with the NIS2 regulation. We believe that any regulatory requirements that have to do with specific aspects of risk mitigation controls, digital resilience, contractual or similar aspects to be implemented by CSPs should be included and associated with this standard. This would guarantee the cybersecurity and resilience objectives of these technical solutions or services for any sector that makes use of them within the EU; being more efficient than publishing specific requirements for each sector in sectoral standards (financial with DORA+EBA guidelines, public administrations with ENS, et cetera). Moreover, the above objectives would be guaranteed not only for CSPs, but also for other sectors within the scope of NIS2, which have a similar level of risk, such as the telecommunications sector.

Overall, by interpreting different points in the guide in particular and altogether, it can be concluded that compliance with the requested requirements can only be met by limiting the uses of the cloud to IaaS and PaaS, excluding SaaS, given that for the latter, the solutions suggested are absolutely unfeasible from a technical point of view.
We believe that this results in a very significant reduction of the competitiveness of European companies in the financial sector and in the freedom to choose the technological solutions best suited to their businesses.

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

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

Deadline:	15.07.2024

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
1	1. Introduction 1.1. Purpose	1.1	2	Amendment	The definition of the “critical or important function” does not correspond to the definition of Article 3(22) of DORA Regulation, which is the following: “ ‘critical or important function’ means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law”.	For consistency reasons, we believe the definition in the ECB Guide should be the same one provided in the DORA Regulation.		Publish
2	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions			Deletion	The institution must retain the ability to bring data and applications back on premises. To this end, the institution 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….”.	When naming possible cloud strategies, it is stated that a combination of the whole list should be used, when only one of them can guarantee recovery for the scenario proposed in the same point. The recommendation that combinations of all of them should be used should be removed and the focus should be on whether the possible solution chosen guarantees recovery in the terms specified.		Publish
3	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			Amendment		This situation is particularly relevant in point 2.2.2 (item 5), through the sentence "The institution must retain the ability to bring data and applications back on premises. To this end, institution should consider using technologies that ensure the portability of data and ICT systems, facilitating effective migration while minimising the impact or using a solution specific to an individual CSP....", given that a large part of the current SaaS services on the market cannot be migrated on premises; a situation that will increase in the future, given that when manufacturers start offering their solutions in SaaS mode, they tend to stop providing the equivalent situation on premise or to reduce their functionality. There are also many services that have been born in SaaS mode and have never had an on-premise version. In the case of applications designed and developed by organisations directly in the cloud (cloud-native applications), the complexity and cost involved in making a technological platform capable of hosting these cloud-native applications available on-premise make the strategy of implementing new applications or modernising existing ones directly in the cloud unfeasible in practice for most organisations.		Publish

4	2.4 Exit strategy and termination rights 2.4.1 Termination rights			Amendment		New requirements in contractual clauses related to termination rights and exit plans. In the first paragraph, reference is being made to the ECB's understanding of general termination rights and lists that such termination rights "could", inter alia, include "an excessive increase in expenses under the contractual arrangements that are attributable to the CSP" next to "ongoing inadequate performance" and "serious breaches of the contractual terms, or of the applicable law or regulations". We note in this context that while ongoing breaches and (even only) one-time serious breaches are usual and market standard termination rights in service agreements (i.e., points (i) and (ii) as listed in the first paragraph), a general termination right due to "an excessive increase in expenses" is unusual since pricing is – next to the service description – a core element of any service contract and as such has to be negotiated and agreed by both Parties. Therefore, an "excessive increase in expenses" should not happen unilaterally and thus such termination right is usually not needed and thus not usually included by default in such agreements. The RTS to specify the policy on ICT services performed by third parties (Art.28.10 of DORA) that were published in March 2024 did not include some of the requirements set out in the revised guidance. For example, there is a request for termination rights for excessive incremental costs attributable to the CSP, or the obligation to regularly review the best options provided for in the exit plans. Given that the negotiation of contractual aspects is a complex process, especially when one of the parties is a large cloud service provider, these types of new requirements should be reflected in the Directive and not in the Guide, so that entities have a better negotiating leverage point, otherwise these requirements are almost impossible to negotiate when it comes to finalising the clauses. With regard to "exit under pressure", it is outside the sphere of influence of institutions when there is a conflict with non-EU legislation, to which CSPs are subject, because this is a political issue.		Publish
5	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs			Amendment		On the effectiveness of the certifications presented by the CSP (issued by third parties). This point highlights the possible weaknesses in terms of the validity of certifications issued by third parties. On the other hand, it is admitted that, in addition to the guarantees of having the possibility of carrying out internal audits of the provider, this can be subcontracted by an entity or group of entities to a third party, which could lead to entities contracting the same third party that carried out the review that led to the certificate being obtained. It would be more efficient to make progress in defining for the whole sector which companies and with what framework and depth these cloud services should be audited, making it compulsory, if necessary, for the auditing companies themselves to be certified as cloud services auditors, and for their review work to be issued, as a result of this certification and specific review framework, with sufficient guarantees of confidence for both institutions and supervisors. Such a solution exists for example with the US SOC II framework, which enjoys a guarantee of confidence for all parties. Such an approach would avoid inefficiencies and high costs for all European institutions and for the cloud service providers themselves.		Publish
6	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details			Amendment		We consider it a great support to have the standard contract clauses developed by public authorities for specific services, as included in the guidance and in Article 30(4) of DORA, however, as of today, except for the core clauses of Article 30. We consider its publication well in advance of the entry into force of DORA very positive, as entities will be required to renegotiate a large part of the contracts to include the requirements of DORA. This process could be carried out more efficiently if we had them.		Publish

7	Box 2: Contractual clauses		16	Amendment		The third point refers to on-site-audits and proposes to deal with the costs of on-site audits via “standard contractual clauses”. We note in this context that we understand the reference to “standard contractual clauses” as meaning that the contract drafters should have available a set of standard clauses that should be used by default when entering into relevant contractual documentation. In our view the use of such standard clauses is good practice in the area of contract drafting and banks are already working with such standard clauses also with regard to requirements that were already raised in the past (e.g. in the context of resolution resilience of service contracts). The side benefit of such use is that it helps to streamline and facilitate the drafting and negotiation of contracts. However, experience also shows that the drafting of such clauses poses some challenges since they should at the one hand be detailed enough to provide clear guidance on what the respective parties want to agree on, and on the other hand should be drafted general enough to allow for a wide-spread use and in order to make them future-proof so that they need not be changed every other month. We thus usually avoid going into too much detail and rather agree on general principles – like, e.g., who bears what costs, are some costs already included in the fees, et cetera.		Publish