EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company

Austrian Federal Economic Chamber - Division Bank and Insurance

Contact person

Mr/Ms

First name

Surname

Email address

Telephone number

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

General comments

Relationship between outsourcing and ICT services

The ECB Guide in a holistic approach tackles both, requirements set forth under the EBA Guidelines on Outsourcing as well as under DORA. Even though DORA aims to harmonize the requirements for outsourcings in the ICT environment (c.f. recital 29 et seq DORA), it needs to be stated, that not every DORA-relevant CSP automatically is to be qualified as outsourcing within the meaning of the EBA Guidelines on Outsourcing and that DORA itself establishes different requirements depending on whether a function is to be qualified as critical or non-critical (c.f. Art 30 para 2 and 3 DORA; e.g post-termination assistance which is only required for critical functions pursuant to Art 30 para 3 lit f DORA).

This shall also be considered with regards to the statement made in para 1.2 of the ECB guide, which states that DORA shall take precedence over this ECB Guide as well as over the EBA Guidelines on Outsourcing.

Before this background, we suggest to either add a clarification that the ECB Guide is applicable to CSP which are to be qualified as Outsourcings within the meaning of the EBA Guidelines on Outsourcing as well as critical functions within the meaning of DORA, or that the applicability of the different expectations need to be assessed on a case-by-case basis, depending on the qualification of the CSP at hand.
2.Reference to NIS2-Directive

The ECB Guide makes reference to provisions of NIS2-Directive when specifying the framework of technical and operational measures to be taken by financial institutions. However NIS2-Directive provides for an exemption from its scope of application for entities falling under sector-specific legal acts, such as DORA for financial entities (c.f. Art 4 NIS2-Directive and Art 1 para 2 DORA). Therefore, instead of the provisions of NIS2-Directive, only the requirements of DORA are applicable for financial entities as lex specialis. Any reference to NIS2 should thus be deleted in the ECB Guide.

3.Principle of Proportionality and Intragroup Arrangements

Art 4 of DORA stipulates the proportionality principle, meaning that financial entities shall implement DORA taking into account their size and overall risk profile as well as their nature, scale and the complexity of their services, activities and operations. While stating the ECB expectations as well as their best practices, the principle of proportionality has completely been disregarded. In contrast, all requirements and expectations are provided on a very detailed level. Moreover, the fact that such cloud services may also be outsourced on an intragroup-basis is also disregarded. As a result, many of the ECB expectations and best practices may be gold-platting (e.g. the requirement to have a monitoring tool independent from the CSP).

We therefore suggest to add a general remark, that the ECB guide shall be read in the light of the principle of proportionality, in particular when receiving cloud services from other intragroup companies.

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		2.3.4.1.			4.Standard of care Across the ECB guide (e.g. in para 2.3.4.1) ECB refers to certain measures as “good practice”. Usually, when describing implementation measures, reference is made to a “best practice” approach, i.e. a best case scenario. With the usage of “good practice”, it could now be understood that this is the “ordinary way” to implement / transpose ECB’s expectation, therefore making it a minimum standard of care. We therefore ask to overthink this increase of standard of care or otherwise provide a concrete definition what is meant under “good practice” (and “best practice”) from ECB point-of-view.		,	Don't publish

2		2.2.1.			5.Responsibility of Management Board Art 5 para 2 DORA provides with the responsibilities of the management of a financial entity with regards to the ICT risk management framework. Lit a) is just stating that the management body shall bear the ultimate responsibility for managing the financial entity's ICT risk. In para 2.1.1 of the ECB guide, this responsibility is being extended so that practically the management body would not only bear the ultimate responsibility for the financial entity but also for every CSP it is contracting ("[…] 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). This statement is based on ECB's understanding of Art 28 para 1 lit a DORA, which just says that financial entities "remain fully responsible for compliance with, and the discharge of, all obligations under this Regulation and applicable financial services law". As stated above, Art 5 para 2 lit a however only refers to the financial entity's ICT risk. The wording of Art 28 para 1 lit a DORA is commonly used in outsourcing context (e.g. in para 35 of the EBA-GL on Outsourcing) and is just referring to the scope of activities, which cannot be outsourcing. ECB's interpretation is exceeding, as it could be understood that the management board shall monitor the ICT risks of its CSPs with the same diligence as its own. Such interpretation would also fail due to the factual and practical circumstances, as contractual rights (e.g. audit, exit etc) have a limited scope and in any case cannot directly influence the actions of management bodies of CSPs (and e.g. overrule shareholder instructions). Furthermore, it needs to be considered that usually CSPs are providing cloud services to more than one principal and therefore the CSP's ICT risk is often dominantly influenced by the total scope of activities, unknown to a single financial entity. Before this background, we suggest to clarify, that the management body of a financial entity fulfills its obligations with regards to the ICT risk of its CSPs by monitoring it through the use of its contractual rights (Art 30 DORA), but not with the same level of diligence as its own ICT risks.		,	Don't publish