EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company

Federal Office for Information Security, Section T 22 - Cloud Security

Contact person

Mr/Ms

Mr

First name

Patrick

Surname

Grete

Email address

patrick.grete@bsi.bund.de

Telephone number

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

General comments

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	Clarification	The statement in the second last pragraph of subsection 2.2.1 is not feasable for all kinds of cloud usage. It applies to mere lift-and-shift scenarios, i.e. where physical servers are moved to cloud but they do not apply to contemporary cloud usage where workload is redesigned for cloud usage. This redesign also affects internal processes of the supervised entity, e.g. for IT-operations. In short: A supervised entity shall assess to which extend it is possible to extract data (and where possible, this shall be tested as the guideline says). But for parts of own IT where there is no possibility of backing up (e.g. serverless applications like AWS Lambda or security functions like CloudTrail; other CSPs have also such services), the BCM strategy becomes much more complex and this shall be mentioned here. The supervised entity must be aware of those parts that cannot be just backed up and has to adopt a well-informed decision when moving to the cloud.	The guideline is not feasible in all cases which might lead to confusion if this is not narrowed to the applicable cases.	Grete, Patrick	Publish
2	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.2	6	Amendment	Please change "Multiple datacenters in different geographical regions" to "Multiple datacenters or availability zones (that consists of different datacenters) in different geographical regions.	The actual phrasing is to vague (it starts with datacenters and ends with availablitiy zones), hence this editorial change	Grete, Patrick	Publish

3	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.2	6	Amendment	Please add in a new bullet point the CAP theorem (https://en.wikipedia.org/wiki/CAP_theorem) in order to keep everybody aware that it is impossible (in a strict scientific and mathematical sense) to build a solution that is always consistent, available and partition tolerant at the same time. Hence strategic decisions and orders of supervising authorities should not demand what is impossible	Keeping everybody aware of things that are impossible (although desirable) is very important for bold guidelines.	Grete, Patrick	Publish
4	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Deletion	In the last bullet point before paragraph 2.2.3, everything after "would expect in an orderly transition under the exit plan." shall be deleted. The meant text describes a situation where an institution is just using some cloud in a lift-and-shift scenario. Moving to cloud is in most cases a transformation process. Infrastructure becomes code, duties fullfilled by servers may be done by serverless functions, AI services are used that are much to expensive to be build onprem, monitoring functions that are to expensive onprem may be used (and lead to more security) to mention just a few aspects. Demanding institions to "retain the ability to bring data and applications back on-premises" is demanding them to not use the full power of cloud services. It also implies that staff must be retained in institutions to operate all IT back in on-prem infrastructure if needed in extreme scenarios which will cost a lot and lead to systematic disadvantages for old institutions with an on-prem IT in comparison to younger supervised institutions that already started with a cloudified IT. It is absolutely clear that the first part of the bullet point is of utmost importance and institutions shall be very aware of their dependencies and shall document those well-informed decisions. The clear risk that a CSP turns off the service abruptly is not a risk that can be fully mitigated within supervised institutions. If this is done - like in the text that shall be deleted - this leads to large unwanted side-effects sketched above. One may also conclude that this risk is of such outstanding importance for EU society to survive that additional legislation is needed (e.g. for taking over the EU-parts of CSPs or other extreme measures)	If the text stays in the guideline severe unwanted side effects will occure.	Grete, Patrick	Publish

5	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	2.3.1	9	Amendment	In the second bullet point, please refer to contemporary standards for cryptographic algorithms, key-lenghts, etc.. Otherwise this is to vague and lead to more questions. E.g. the technical guidelines from the German BSI are updated on an annual basis and can be found here: https://www.bsi.bund.de/dok/TR-02102-en Please add them inline or as a footnote	Relevant, usable and annually updated content improves the usability of the guideline	Grete, Patrick	Publish
6	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data	2.3.2	10	Clarification	Please add the following sentence at the end of the first paragraph: "If the institution is already working in other countries (even outside the EU), then using a CSP in that country normally does not lead to much more additional threats since that instution is already forced to comply with local laws so that search warrants, law suits etc that may apply to the CSP will also apply to the institution itself."	The clarification gives more guidance to the reader	Grete, Patrick	Publish
7	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	Clarification	It is unclear to me what is the content of the individual clauses the institution shall agree with the CSP. Normally, the CSP provides the Self-Service-Portal for all users and the institution can configure the service as they wish without personal interaction with the CSP. Please clarify what is meant here	If this is not further clarified, the reader will not know what EZB intention is which will lead to more questions	Grete, Patrick	Publish
8	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	2.3.4.2	11	Amendment	Please add another bullet point reading: "Usage of priviledged access to institutions workload shall (where technically feasible) be monitored and the monitoring data shall be continuously analyzed for indicators of compromise. Such findings shall trigger Security alarms.	This adds further value to the guidance and enhances the security level	Grete, Patrick	Publish