EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
ABBL - The Luxembourg Bankers' Association

Contact person

Mr/Ms
Mr

First name
Andrey

Surname
MARTOVOY

Email address
digital@abbl.lu

Telephone number
00 352 46 36 60 501

☐ 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	1. Introduction 1.1. Purpose	2	2	Amendment	Additional prescriptive guidance on cloud-specific outsourcing risks is not needed given current EU regulatory frameworks such as DORA and the EBA Outsourcing Guidelines. DORA specifically contemplates the types of risks associated with ICT third-party service providers, such as cloud providers, and sets out enhanced and harmonised risk management requirements, alongside an oversight framework that industry expects will capture those Cloud Service Providers (CSPs) that pose the most significant threat to the stability of the financial sector.	The supervisory expectations set out in the Guide go well beyond the risk management requirements set out in both DORA and the EBA Outsourcing Guidelines in a number of areas, without necessarily addressing any purported deficiencies in current resilient frameworks or existing risk-management practices. The ECB's Guide further complicates the sector's implementation of DORA's requirements by introducing additional requirements and contractual remediation, and it will lead to fragmentation within the EU, instead of contributing to the harmonisation and consolidation of regulatory requirements and supervisory expectations.	MARTOVOY, Andrey	Publish
2	1. Introduction 1.1. Purpose	Definitions	2	Amendment	Given the Guide is intended to reflect the ECB's understanding of DORA's requirements, alignment with the DORA's critical or important functions (CIFs) definition would provide welcomed clarity and consistently for industry in meeting supervisory expectations.	The Guide should align with DORA definitions and scope to provide consistency for financial institutions (FIs) dealing with overlapping frameworks and supervisory expectations and to support DORA's harmonisation objectives.	MARTOVOY, Andrey	Publish

3	1. Introduction 1.2 Scope and Effect	1	3	Amendment	The Guide applies the proportionality and risk-based principles embedded in DORA inconsistently throughout – applying expectations for risk-management of service providers and subcontractors that support CIFs to certain requirements, but not others. It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity.	The Guide should ensure a consistent application of proportionality which takes into account the nature of the cloud service, the complexity of the outsourced functions, the risks arising from the outsourcing arrangement, the criticality or importance of the outsourced function and the potential impact of the outsourcing on the continuity of their activities.	MARTOVOY, Andrey	Publish
4	1. Introduction 1.2 Scope and Effect	General	General	Amendment	Where the Guide intends to capture subcontractors, it should explicitly apply a materiality threshold to supply chain scope (in alignment with DORA). Without the consistent application of a risk-based approach, the supervisory expectations in the Guide could be interpreted as applying to a very expansive scope of CSPs and their subcontractors. This further complicates the interpretation and application of the Guide's supervisory expectations consistently with DORA and the EBA Guidelines.	The Guide should apply an appropriate materiality threshold to supply chain scope that is aligned with DORA and the regulatory technical standard on subcontracting (i.e. subcontractors that effectively underpin services supporting a critical or important function) to uphold a consistent approach that is feasible and reflects proportionality.	MARTOVOY, Andrey	Publish
5	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business	1	6	Deletion	The Guides consistently references the NIS2 Directive for interpretation even if there are equivalent requirements included in DORA. As DORA is *lex specialis* to NIS2, these references should be removed.	DORA is *lex specialis* to NIS2 and therefore all references to interpretation by the ECB of NIS2 should be removed.	MARTOVOY, Andrey	Publish
6	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question	3	4	Amendment	Risk management and contractual frameworks between FIs 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.*	It is not appropriate for third-parties to establish "equivalent" risk management practices to a financial entity. This expectation goes beyond current regulatory expectations and reasonable risk management practices	MARTOVOY, Andrey	Publish
7	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	4	4	Clarification	The requirement to: - ***"assess the CSP's ability to provide the information required for these checks"*** lacks clarity; - ***"ensure that the CSP has itself properly implemented the relevant checks"*** lacks clarity and should be reframed as "***assess that..***"; - consider "***the risk of a considerable fall in quality***", is subjective and not feasible at the pre-contractual stage. This risk is managed through contractual provisions and the ongoing monitoring process addressing service level quality and performance. - consider "***the risk of a significant increase in price***" is not feasible at the pre-contractual stage. This risk is managed through contractual provisions. - consider "***the risk of a significant increase in price***" is not feasible at the pre-contractual stage. This risk is managed through contractual provisions.	The ECB guide expands requirements above the scope of DORA and EBA GLs, without additional benefit to risk management, and does not adequately apply a risk based approach. Additionally, it would not be feasible to address a number of the risk considerations at the pre-contractual phase. Many also lack clarity and/or are subjective.	MARTOVOY, Andrey	Publish

8	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2	6	Deletion	The suggestion that back-ups of CIFs should not be stored in the cloud service provider that hosts the services will not always be practically possible or in the best interests of the institution and its resilience. There are several technical difficulties with storing back-up data in a different CSP: - For any service which uses or is native to the CSP, the data format will not allow for use in another CSP or another equivalent service without conversion. For example, data stored in one CSP using their storage solution would not be usable within the storage solution in another CSP. If the original CSPs storage solution is proprietary then conversion of the data would be required before it could be used. This can be difficult and can take significant time making its use in a recovery or resilience scenario limited. - It is also possible that a native tool is not designed for the data to be extracted. In these cases, a requirement to have backup in another CSP would prevent the use of certain CSP-native tools. - In the scenario of a complete outage, data stored in another CSP would take significant time to get transfered back to the original CSP. The amount of data is increasing exponentially. When data reaches the scale of petabytes, digital means of transfer begin to become impractical and it becomes necessary to explore the physical transport of data between premises. It is also the case that data alone will have limited resilience benefit. Even in an ideal scenario in which the firm had perfect data back-up in an alternative CSP, it would take weeks to build the infrastructure and applications needed to provide the service from that CSP and test their functionality. This means that the financial entity would almost certainly breach its maximum tolerable level of disruption. In a severe scenario, any market-wide impacts resulting from an outage of that financial entity or its services, would not be prevented by maintaining back-up data in another CSP. To achieve the resilience outcome that the ECB seem to be targeting, it would be necessary to maintain live-live functionality across multiple CSPs. This also faces technical limitations, most notably the near impossibility of maintaining data synchronisation across different infrastructures and platforms operating in different geographic locations. It would also preclude the use of cloud-native tooling for which redundancy in a different CSP would not be possible owing to the proprietary nature of the service (this could include most SaaS offerings). Finally, even if the technical challenges could be overcome, the business implications would be substantial. The *de-facto* ban on using cloud-native tooling would significantly undermine the business case for using cloud. It would also be only the best	The requirement to utilise a different CSP for data backup exceeds the EBA/DORA existing requirements. Such a requirement has several drawbacks including extreme technical challenges, limited resilience benefits/use cases, and significant business case impacts for cloud. Pursuing this requirement could limit the viability of using cloud for EU financial entities and create a competitive disadvantage for EU financial services.	MARTOVOY, Andrey	Publish

9	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	6	7	Deletion	The expectation that "***The institution must maintain the ability to bring data and applications back on-premises*** " has caused significant concern among the industry given the technical difficulties with achieving this. For many cloud uses, such as cloud-native tools, bringing the data and applications back on premise would require the financial entity to maintain comparable capabilities as the CSP. Given the tools used may be proprietary, this often not be possible. To use the example from above, data stored using a CSPs storage tool would not be compatible with a storage tool from another CSP or what the financial entity maintains on premise. Moving the data back on presmise in this example would require conversation and significant testing rendering the strategy ineffective for limiting disruption to within agreed tolerance levels. From a resource perspective, maintaining these cloud computing capabilities would not be feasible excpet for perhaps the very largest financial entities. Even then, it would be cost prohibitive for Fis to use cloud under this requirement. This requirement would represent a de-facto ban on the majority of cloud-native tools and would likely significant impact EU financial entities ability to use SaaS offerings. The strategy suggested by the ECB of containerisation and virtual machine based-applications, while technically possible, would equate to treating CSPs as data centre providers. This is likely far below the strategies of most EU FIs and would effectively erode the value added of cloud computing which has led to such wide-spread adoption of the technology. Operating under these limits would see EU financial entities face a significant competitive disadvantage to firms in other markets who will be able to improve the security, resilience and product offerings in a way that EU financial entities will not be able to access. 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***	In many cases, bringing data and applications back on premise will not be viable either technically, or from a business perspective. This requirement would represent a de-facto ban on most cloud-native tools and SaaS deployments, resulting in a significant competitive disadvantage to EU financial institutions for limited to no resilience benefit.	MARTOVOY, Andrey	Publish
10	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	8	Deletion	Whilst it is reasonable to expect the remediation of deficiencies identified during testing, it is unclear how this would be addressed by renegotiating the contract with the CSP. Gaps identified during BCP testing should be addressed in the BCP plan, and the control environment of the CSP.	The suggested guidance to address deficiencies identified during testing through contractual remediation risks creating an undesirable environment of continual off-cycle renegotiations and does not reflect reasonable risk management practice. This also risks undermining contract remediation efforts as part of DORA compliance, which represent a significant operational uplift for financial entities.	MARTOVOY, Andrey	Publish
11	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	4	8	Amendment	The Guide should expressly state that financial entities concentration risk should be assessed on a risk-based approach. DORA does not refer to “data residency” and the inclusion of such term in the Guide could lead to confusion among financial entities. Hence, the second paragraph of 2.2.4 should be amended to indicate: “…alongside aspects of data (to delete the word **"residency"**) location.”	DORA does not refer to “data residency”. In the guide, the term should be replaced with “location”.	MARTOVOY, Andrey	Publish

12	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	5	9	Amendment	The Guide states that, in order to have ICT security within the cloud, that a financial entity should encrypt data ***"in transit, at rest and, where feasible, in use."*** IaaS providers automatically de-crypt data once a user has access to the particular workload in question. Encryption, in this respect, serves no ICT security benefit. The cybersecurity risk associated with encryption from a IaaS perspective relates to access management controls, to which a malicious actor could gain access and would also receive automatic decrypted data. We recommend this requirement is risk-based depending on the cloud service. *2.3: "encryption methods in line with the institution's data sensitivity classification policy, **the type of cloud service and a risk-based approach.**"*	The only security benefit to encryption in an IaaS context is in relation to physical security and a malicious actor stealing a specific physical disk from a server in the data centre of a cloud provider. This constitutes a level of information breach and sophistication that is unrealistic and inappropriate to account for within ECB Supervisory Guidance.	MARTOVOY, Andrey	Publish
13	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data	4	10	Amendment	The Guide introduces requirements that go beyond what is in DORA (recitals 82 and 83), therefore paragraph 1 of Chapter 2.3.2 should be amended. The absence of a clear risk-based approach endangers capturing an inappropriately broad scope of subcontractors. As noted above, all references to subcontractors should explicitly apply a materiality threshold in alignment with DORA (i.e. as ultimately reflected in the final draft regulatory technical standard on subcontracting).	The Guide should apply an explicitly risk-based approach to the requirement to assess data location and processing risks. The reference to "relevant" subcontractors is vague and does not sufficiently apply materiality.	MARTOVOY, Andrey	Publish
14	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	4	11	Deletion	The guidance should focus on what is substantively required, and refrain from prescribing the format and how it should be achieved. Further, this expectation does reflect the reality of how cloud services are configured and contracted for. For instance, cloud services are typically provided for under a framework contract or Master Services Agreement (MSA). It would not be appropriate for an FI to negotiate individual clauses in contracts each time they configure workloads under the overarching contract. It would be more appropriate for the Guide to state that it is *"good practice for institutions to **consider** (to delete the word "agree") individual clauses with the CSP **when entering into a cloud outsourcing arrangement** (to delete the phrase "configuring the cloud environment")."*	The Guide should not dictate or prescribe how FIs should approach contractual arrangements with CSPs, particularly given the way cloud services are typically contracted for. The requirement for FIs to negotiate individual clauses with CSPs should be deleted.	MARTOVOY, Andrey	Publish
15	2.4 Exit strategy and termination rights 2.4.1 Termination rights	4, 5	12	Deletion	The Guide creates new additional termination rights which are too granular and go beyond existing regulatory expectations and contracting best practice. It would be unreasonable to expect the reasons for termination detailed in the guide to be reflected in contractual arrangements with CSPs. In particular, the Guide should not include the following: - ***excessive increase in expenses*** – This is subjective and does not reflect the reality of contracting, which would not allow unilateral changes to fees. - ***the relocation of business units or data centres*** – too granular. This would be captured by material breach termination rights, given existing outsourcing requirements, that providers seek FIs consent ahead of changing the service or data storage locations - ***changes to national legislation or regulations applicable to data location and processing*** – this would be covered by contractual rights to terminate for legal/regulatory reasons under the impediments capable of altering performance concept required by the EBA Guidelines - ***significant changes to the management of cyber risk in the subcontracting chain*** – this is covered by general termination rights related to subcontractors under EBA GLs and DORA - ***failure to successfully execute cloud provider test migrations at agreed times*** – too granular. It is unclear what the material risk is here and material breach termination rights would achieve the same outcome	The Guide specifies non-binding termination rights which do not reflect existing legal or market reality. The expectations go beyond DORA and EBA requirements adding unnecessary confusion and complexity to industry's understanding and application of DORA.	MARTOVOY, Andrey	Publish

16	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	3	15	Amendment	Financial entities may utilise different teams and functions for oversight and monitoring of a CSP due to the nature of the cloud service, the different expertise of various teams, how it operates across multiple financial entities or services and the materiality of the service provided. Enforcement of all monitoring within one function would not utilise the expertise of the financial entity effectively and would require reorganization of well-established functions within financial entities. Oversight and monitoring can be undertaken by individual cloud teams, third party oversight, cybersecurity functions, and technology functions or a combination of colleagues within those teams. We recommend the following amendment: 2.5.1: "… ***supervised institutions should retain expertise in-house (to delete the following phrase: ", with a centralised function or department being recommended for the monitoring of CSPs"). The monitoring…*** *"*	The ECB should not enforce monitoring of CSPs to be undertaken by a single centralised function or a single department within a financial entity.	MARTOVOY, Andrey	Publish
17	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	4	15	Clarification	The guidance should suggest what other tools should be taken into account if the ECB states that monitoring tools provided by a CSP might not be sufficient.	Lack of clarity about ECB expectations without further examples.	MARTOVOY, Andrey	Publish
18	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	3	16	Deletion	The Guide introduces new requirements, beyond those set out in DORA. Therefore, the last sentence of this section which states ***"Institutions should use contractual clauses to ensure appropriate incident and monitoring reports, enabling ongoing assessment of outsourced functions."*** should be deleted.	The requirements that go beyond what is set in DORA	MARTOVOY, Andrey	Publish
19	Box 2: Contractual clauses	4	16	Deletion	We propose the call for Standard Contractual Clauses (SCCs) is dropped given that there is a EU forum already reviewing the issue, and it has not yet produced any standardised clauses. A better approach would be to say that in the contractual arrangement the following bullet points should be considered, potentially via SCCs.	Risk of incoherent approach from EU institutions.	MARTOVOY, Andrey	Publish
20	Box 2: Contractual clauses	8	16	Amendment	The Guidance should state that institutions have taken safeguards against unilateral changes, rather than determining where a separate copy for digital provisions is required for these purposes.	Setting out requirements for particular incidents will create partial coverage. The guidance should be outcomes focused.	MARTOVOY, Andrey	Publish
21	Box 2: Contractual clauses	7	16	Deletion	The recommendation that ***"contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indicating the maximum cost"*** should be deleted. This goes beyond existing practice and the EBA Guidelines in expecting this information to be set out in the contract.	The Guidance should interpret the existing legal obligations, rather than adding to them through new levels of practical prescription.	MARTOVOY, Andrey	Publish
22							MARTOVOY, Andrey	Publish
23							MARTOVOY, Andrey	Publish
24							MARTOVOY, Andrey	Publish
25							MARTOVOY, Andrey	Publish
26							MARTOVOY, Andrey	Publish
27							MARTOVOY, Andrey	Publish
28							MARTOVOY, Andrey	Publish

29							MARTOVOY, Andrey	Publish
30							MARTOVOY, Andrey	Publish
31							MARTOVOY, Andrey	Publish
32							MARTOVOY, Andrey	Publish
33							MARTOVOY, Andrey	Publish
34							MARTOVOY, Andrey	Publish
35							MARTOVOY, Andrey	Publish
36							MARTOVOY, Andrey	Publish
37							MARTOVOY, Andrey	Publish
38							MARTOVOY, Andrey	Publish
39							MARTOVOY, Andrey	Publish
40							MARTOVOY, Andrey	Publish
41							MARTOVOY, Andrey	Publish
42							MARTOVOY, Andrey	Publish
43							MARTOVOY, Andrey	Publish
44							MARTOVOY, Andrey	Publish
45							MARTOVOY, Andrey	Publish
46							MARTOVOY, Andrey	Publish
47							MARTOVOY, Andrey	Publish
48							MARTOVOY, Andrey	Publish
49							MARTOVOY, Andrey	Publish
50							MARTOVOY, Andrey	Publish
51							MARTOVOY, Andrey	Publish
52							MARTOVOY, Andrey	Publish
53							MARTOVOY, Andrey	Publish
54							MARTOVOY, Andrey	Publish
55							MARTOVOY, Andrey	Publish
56							MARTOVOY, Andrey	Publish

57							MARTOVOY, Andrey	Publish
58							MARTOVOY, Andrey	Publish
59							MARTOVOY, Andrey	Publish
60							MARTOVOY, Andrey	Publish
61							MARTOVOY, Andrey	Publish
62							MARTOVOY, Andrey	Publish
63							MARTOVOY, Andrey	Publish
64							MARTOVOY, Andrey	Publish
65							MARTOVOY, Andrey	Publish
66							MARTOVOY, Andrey	Publish
67							MARTOVOY, Andrey	Publish
68							MARTOVOY, Andrey	Publish
69							MARTOVOY, Andrey	Publish
70							MARTOVOY, Andrey	Publish
71							MARTOVOY, Andrey	Publish
72							MARTOVOY, Andrey	Publish
73							MARTOVOY, Andrey	Publish
74							MARTOVOY, Andrey	Publish
75							MARTOVOY, Andrey	Publish
76							MARTOVOY, Andrey	Publish
77							MARTOVOY, Andrey	Publish
78							MARTOVOY, Andrey	Publish
79							MARTOVOY, Andrey	Publish
80							MARTOVOY, Andrey	Publish
81							MARTOVOY, Andrey	Publish
82							MARTOVOY, Andrey	Publish
83							MARTOVOY, Andrey	Publish
84							MARTOVOY, Andrey	Publish

85							MARTOVOY, Andrey	Publish
86							MARTOVOY, Andrey	Publish
87							MARTOVOY, Andrey	Publish
88							MARTOVOY, Andrey	Publish
89							MARTOVOY, Andrey	Publish
90							MARTOVOY, Andrey	Publish
91							MARTOVOY, Andrey	Publish
92							MARTOVOY, Andrey	Publish
93							MARTOVOY, Andrey	Publish
94							MARTOVOY, Andrey	Publish
95							MARTOVOY, Andrey	Publish
96							MARTOVOY, Andrey	Publish
97							MARTOVOY, Andrey	Publish
98							MARTOVOY, Andrey	Publish
99							MARTOVOY, Andrey	Publish
100							MARTOVOY, Andrey	Publish
101							MARTOVOY, Andrey	Publish
102							MARTOVOY, Andrey	Publish
103							MARTOVOY, Andrey	Publish
104							MARTOVOY, Andrey	Publish
105							MARTOVOY, Andrey	Publish
106							MARTOVOY, Andrey	Publish
107							MARTOVOY, Andrey	Publish
108							MARTOVOY, Andrey	Publish
109							MARTOVOY, Andrey	Publish
110							MARTOVOY, Andrey	Publish
111							MARTOVOY, Andrey	Publish
112							MARTOVOY, Andrey	Publish

113							MARTOVOY, Andrey	Publish
114							MARTOVOY, Andrey	Publish
115							MARTOVOY, Andrey	Publish
116							MARTOVOY, Andrey	Publish
117							MARTOVOY, Andrey	Publish
118							MARTOVOY, Andrey	Publish
119							MARTOVOY, Andrey	Publish
120							MARTOVOY, Andrey	Publish
121							MARTOVOY, Andrey	Publish
122							MARTOVOY, Andrey	Publish
123							MARTOVOY, Andrey	Publish
124							MARTOVOY, Andrey	Publish
125							MARTOVOY, Andrey	Publish
126							MARTOVOY, Andrey	Publish
127							MARTOVOY, Andrey	Publish
128							MARTOVOY, Andrey	Publish
129							MARTOVOY, Andrey	Publish
130							MARTOVOY, Andrey	Publish
131							MARTOVOY, Andrey	Publish
132							MARTOVOY, Andrey	Publish
133							MARTOVOY, Andrey	Publish
134							MARTOVOY, Andrey	Publish
135							MARTOVOY, Andrey	Publish
136							MARTOVOY, Andrey	Publish
137							MARTOVOY, Andrey	Publish
138							MARTOVOY, Andrey	Publish
139							MARTOVOY, Andrey	Publish
140							MARTOVOY, Andrey	Publish

141							MARTOVOY, Andrey	Publish
142							MARTOVOY, Andrey	Publish
143							MARTOVOY, Andrey	Publish
144							MARTOVOY, Andrey	Publish
145							MARTOVOY, Andrey	Publish
146							MARTOVOY, Andrey	Publish
147							MARTOVOY, Andrey	Publish
148							MARTOVOY, Andrey	Publish
149							MARTOVOY, Andrey	Publish
150							MARTOVOY, Andrey	Publish