EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company

ECIIA (European Confederation of Institutes of Internal Auditing)

Contact person

Mr/Ms

Vandenbussche

First name

Pascale

Surname

Email address

p.vandenbussche@eciia.eu

Telephone number

+32.491.10.44.98

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

General comments

We thank the ECB for the opportunity to comment - and welcome the guidance that will assist internal auditors in planning audits on cloud services usage and relevant providers. In general, the guidance assists organisations build the necessary control environment to mitigate risks associated with the usage of cloud.
ECIIA is the professional representative body of 34 national institutes of internal audit in the wider geographic area of Europe and represent 55.000 members.
ECIIA is the the consolidated voice of the profession of internal audit and aims representing and developing the internal audit profession as part of good corporate governance, by achieving thought leadership through publications on relevant topics and by interacting with the Regulators, as required, and any other appropriate institutions of influence at European level.

Role of Internal Audit

The role of internal audit is substantial in managing the risks associated with the usage of cloud services. Especially in regards to broad risk assessments which are integral to decisions being made to shift applications to the cloud and select software, platforms or infrastructure of cloud service providers. On that note, cloud providers should also perform risk assessments of their services and use the insights from internal auditors as part of this exercise. Internal audit as part of our 3rd Line responsibilities, provides assurance on cloud readiness assessments of existing vendor procurement and contract processes, and identify cloud control gaps. By reviewing the risk framework based on identified cloud risks, internal audit assists organisations in understanding and mitigating these risks. Internal audit will also assess data governance programs and ensure that regulatory requirements have been applied. Internal audit continues to be engaged in risk discussions, along with the organisation's security, risk, and compliance groups.

Technical Guidance and Best Practices

As this guidance covers certain technical topics, we advise to include more best practices (as in the section 2.3.1) to better illustrate the ECB's expectations.
Clear definitions of the governance framework (we recommend to use the 3 lines model*), including the roles, responsibilities, and oversight of the 1st and 2nd lines alongside the one of internal audit are crucial.

Interactions with Cloud Service Providers

Obtaining detailed, accurate and complete information from the CSPs is a challenge for all Financial Service Entities, including their internal audit functions. Although audit rights are included in contracts, necessary information from CSPs is not always forthcoming. Therefore, we recommend the ECB to specify the minimum audit requirements for services not impacting critical/important functions. Including best practices for situations where support from CSPs is lacking would also be beneficial.

General Recommendations

As a general comment, the ECB should consider enhancing its description of the mandatory work expected from the internal audit function for different types of cloud outsourcing services. We recommend clear definitions on key topics such as "critical functions", "undertaking", the different kinds of cloud categories, "major disruptions" and "assets". Although DORA includes definitions for many of these topics, the guidance references should be clearly stated.

Conclusion

In conclusion, as outsourcing cloud services becomes increasingly more complex, robust governance, clear definitions and explicit expectations are required from the ECB to assist Financial Institutions in managing and reducing associated risks. Internal audit is well-positioned to add value to the organisations and to audit the CSPs individually or as part of a pooled approach.

We remain at disposal for any further discussions and our detailed comments are included in the second spreadsheet.

M. Turconi-ECIIA President and A. Bracht-ECIIA Vice President

*:3 lines model: https://www.theiia.org/en/content/articles/global-knowledge-brief/2020/july/the-iias-three-lines-model/

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	1	Clarification	What are general controls that should always be covered through cloud audits - and what are the specific controls for specific services?	A clear requirement will facilitate getting the right information/data from the CPs	ECIIA	Publish
2	1. Introduction 1.1. Purpose	1.1	2	Amendment	The use of the word "undertaking" in the definitions of private and community cloud is inconsistent with the definitions provided in the Guidelines for Outsourcing Arrangements and in those commonly used (e.g. from NIST). It should be substituted with "business", "enterprise" or "institution"	We must avoid uncertainties in the definition	ECIIA	Publish

3	1. Introduction 1.1. Purpose	1.1	2	Clarification	The ECB's definition of critical or important functions reported in the section "Definitions of terms for the purposes of this Guide" is: "Activities, services or operations whose discontinuance is likely to lead to disruptions of services that are essential to the real economy in one or more member states or the disruption of financial stability, given the size, market share, external and internal interconnectedness, complexity or cross border nature of an institution or group's activities, particularly as regards the substitutability of those activities, services or operations." It should be confirmed that for the purposes of this Guide, critical functions are only those from which systemic impacts may arise.	Critical functions are a key theme of the guidance. It is important to have a clear definition to guarantee correct implementation.	ECIIA	Publish
4	1. Introduction 1.1. Purpose	1.1	2	Amendment	We suggest to align the definition of "ICT asset" to the definition contained in DORA: "a software or hardware asset in the network and information systems used by the financial entity"	DORA is a key regulation and we see big advantages to align definitions between DORA and this guidance.	ECIIA	Publish
5	1. Introduction 1.2, Scope and effects	1,2	4	Amendment	We suggest to change the sentence "Where a non-CSP third-party provider (TPP) is reliant on cloud services provided by a CSP, the same supervisory expectations apply. " and add only for outsourcing of critical functions	The scope is too large and to difficult to manage.	ECIIA	Publish
6	Chapter 2.1 Governance of Cloud Services 2.1.1 Full Responsibility	2.1.2	4	Clarification	The sentence Consequently, institutions should ensure that their CSPs have established equivalent risk management practices, processes and controls" is unclear.	We can not force CPS to implement risk framework and what are the ECB expectations here.	ECIIA	Publish
7	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2,1,2	5	Clarification	The sentence "• perform thorough analysis of the control processes that will be established" is unclear	ECB expectations should be better defined	ECIIA	
8	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Amendment	The sentence "assess the CSP's ability to provide the information required for these checks;" should be modified as follow: "assess that the CSP has properly implemented relevant checks;"	We believe that the proposed sentence is not clear enough.	ECIIA	Publish

9	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Amendment	Since the environment provided to the credit institution can be hosted anywhere in the planet we recommend to add: •The possibility of a credit institution to select the geographical area to store data •The compliance of the CSP with the local regulations that may apply •The practices applied for continuous monitoring of the regulatory framework as well and periodic assessment	The points could be also considered in the pre-outsourcing analysis	ECIIA	Publish
10	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2	5	Clarification	It is unclear what the phrase "the risks of a multi-tenant environment" means in the context of a pre-outsourcing assessment	We recommend a clearer definition	ECIIA	Publish
11	Chapter 2.1 Governance of Cloud Services 2.1.3. Consistency between an institution's cloud strategy and its overall strategy	2.1.3	5	Clarification	There seems to be a broadening of the concept reported in DORA, which requires the definition of a strategy limited to ICT third-party risk management. In the Guide, the ECB seems to require a strategy that includes, in addition to risks, also business elements / operating service model. It is therefore important to specify that the concept of outsourcing strategy is limited to strategy on ICT third-party risk as stated in DORA. It also needs to be clear on who should approve the cloud strategy, e.g. Board. and how often.	We recommend to align with DORA requirements or clearly specify the deviations required.	ECIIA	Publish
12	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2,2	6	Supportive	Current regulations strengthen the idea of having good business continuity plans and adequate testing plans. This forces entities to stress their test models on *on-premise* systems with data in provider's cloud. We welcome the idea to strengthen t that entities get involved in carrying out and obtaining the results of the tests carried out by cloud providers.		ECIIA	

13	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	This provision could implicitly introduce new requirements, while referring to the concept of a Holistic Perspective. Whenever the expectation is to consider both Business Continuity (Backup/Restore) and Exit Strategy elements in a unique framework, we foresee a potential risk in a dramatic increase in complexity, significantly limiting the architectural alternatives to be considered and further complicating the verification and control actions towards CSPs. There seems also to be in certain cases some ambiguity about whether backup is required for data only or for systems (which is completely different in terms of impact). In particular: In the first part of the paragraph the focus is on data while in the following part the backup procedure involve also critical or important systems.	It could imply new requirements, compared to current best practices. The requirements must be clear for business continuity and exit strategy elements. Different frameworks should apply.	ECIIA	Publish
14	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	In our understanding the backups could reside on a different network architecture (physically and logically segregated from the source ICT system), even if it belongs to the same CSP, and not necessarily be implemented on a completely different CSP. Please note that the measure to have back-ups stored in other cloud providers seems to be not applicable for SaaS Cloud and in any case would imply a huge effort with direct impact on the cloud benefits. In addition, it should be noted that the CSP ensures the BC through redundancy not through a backup system and that the article 12 of DORA refers in general to TPP (not specific to CSP).	We recommend to be clearer as DORA does not cover this aspect.	ECIIA	Publish
15	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	Delete	The paragraph collapses Business Continuity and Exit Strategy considerations and introduces the concept of an "exit under stress or an exit without the cooperation of the CSP(s)". We believe this requirement is quite impossibile to be respected, a recovery for continuity purposes should happen in hours while an exit takes months. The only way this could be achieved would be to develop, matain and keep at scale different parallel systems performing the same functions using different architectures and infrastructure, that would mean to double costs and maintenance effort.	We recommend to illustrate with best practices or delete in order to be able to fulfill the obligations	ECIIA	

16	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	6	Clarification	"multiple data centers" needs to be clarified what is deemed to be a data centre, and to what tiering (e.g. Tier IV, III etc..). AWS viewed Availability Zones (AZ) as Data Centres, but the US-East 1 outage incident details exposed information that suggested Azs are not on par with on-prem Bank data centre resilience capabilities.	ECB must clarify to avoid misunderstanding	ECIIA	Publish
17	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	6	Amendment	"A multi-region approach" makes an assumption that multi-region enhances security, however, it doesn't handle data privacy laws. This should include a statement to caveat where it doesn't breach laws etc..	It is important to make sure that laws are not breached	ECIIA	Publish
18	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	Footnote 7	7	Deletion	The guide in this chapter refers to the EBA guidelines in footnote 7 to define critical functions. We suggest to eliminate this reference to maintain consistency with the definitions provided in the table "Definitions of terms for the purposes of this Guide" on page 2.	We recommend uniformity in the definitions	ECIIA	Publish
19	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2	7	Amendment	"as defined in the institution's internal policies" Plus laws, regulatory rules and regulations in case internal policies have not been considered.	Suggestion to complete the requirements	ECIIA	Publish

20	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 expectation "The institution must maintain the ability to bring data and applications back on-premises" is overly limiting - especially when it comes to the use of SaaS solutions - and could hinder the scalability of solutions and the adaptability/flexibility of the institutions themselves. 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 ability to bring data and applications back on-premises" or alternatively rewording it in line with the regulatory provisions as follows: "The institution must maintain the ability to bring data and applications back on-premises or transfer them to alternative CSPs or back-up providers"	Suggestions to better align with DORA requirements	ECIIA	Publish
21	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	"On the basis of these provisions, the ECB understands that an institution should test its CSP's disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications" We suggest to modify as follows: "with reference to IasS Cloud test disaster recovery plans and should not rely exclusively on relevant disaster recovery certifications"	Specifications should be added	ECIIA	Publish
22	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	We suggest to amend the sentence "When conducting disaster recovery tests with the CSP, the institution should perform spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event." as follows: "When conducting disaster recovery tests with the CSP, the institution, where possible, may perform spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event"	Specifications should be added	ECIIA	Publish

23	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	It should be clarified by Authorities what would constitute a meaningful concentration of services in a specific location or in a specific function/service, or how much weight should be given to the assessed concentration risk. In fact, it has to be considered that minimizing concentration could incur in significant trade-offs in matters of system complexity, performance and cost.	We suggest to clarify the concentration concept	ECIIA	Publish
24	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	In the section "When performing risk assessments, the ECB considers it good practice to scrutinise typical risks relating to cloud services " clarification needs to be made to establish clear responsibilities towards the three lines.	We recommend to clearly define the responsibilities in the organisation.	ECIIA	Publish
25	Chapter 2.3. ICT security, data confidentiality and integrity	2.3	9	Delete	We suggest to delete "Consequently, institutions need to protect their data (including relevant back-ups) from unauthorised access by maintaining high levels of data encryption and constantly adapting to external threats. This involves encrypting data in transit, at rest and, where feasible, in use, employing appropriate encryption methods in line with the institution's data sensitivity classification policy. "	We suggest to rely on existing minimum standards of data encryption	ECIIA	
26	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	9	Amendment	"of data in transit and data at rest "should include data in use i.e. memory.	We suggest an extension to the text	ECIIA	Publish
27	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	9	Clarification	With reference to envisaged "good practice for institutions to restrict the locations where CSPs can store their data" it has to be noted that when dealing directly with a CSP - as opposed to a TPP - the location is usually an institution's own choice. How shoud this aspect be weighted against considerations of geographical concentration from before?	We see a risk when managing this requirement and the geographical risk described in the guide.	ECIIA	Publish

28	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	Clarification	This reads as best practice and optional, what are the minimum requirements for FS firms t?	It is unclear.	ECIIA	Publish
29	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	10	Clarification	On responsibilities in controlling the cryptographic keys. Can companies revoke the data from the CSP after exiting the business relationship so that the CSP doesn‘t have access to the data anymore?	It is unclear.	ECIIA	Publish
30	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 Final paragraph	10	Clarification	Please clarify how the listed security measures can strengthen data security on cloud environment.	It is unclear.	ECIIA	Publish
31	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	Will the ECB regulate the CSPs and without this, the FS firms may not be able to get all relevant information?	Concern to be able to get the relevant information from the CPS.	ECIIA	Publish

32	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	2.3.3	10	Clarification	in relation to the provision "adopt a clear policy on the classification of all ICT assets, including those that are outsourced to CSPs", clarification is needed from the ECB on the definition of an ICT asset within Cloud services	A clear definition is required.	ECIIA	Publish
33	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	Instead of "Roles and Responsibilities", "Roles and responsibilities for Identity & Access Management"is sugested.	We suggest a broader title aligned to the content.	ECIIA	Publish
34	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	we suggest the following change in the sentence "The ECB considers it good practice for institutions to agree individual clauses with the CSP regarding the configuration of the cloud environment"	We suggest clearer requirements.	ECIIA	Publish
35	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	12	Amendment	"monitoring tools" should become "monitoring „and logging" tools"	We suggest clearer requirements.	ECIIA	Publish
36	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4	12	Best practices	The ECB should better clarify its expectations regarding the exit plans tests that must be carried out. On many occasions it is really difficult to establish very large service tests, not only because of the complexity of organizing and executing them, but also because of their cost. It would be convenient for them to establish what type of tests they require/best practices.	Best practices would help defining the requirements	ECIIA	Publish

37	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4	12	Clarification	With reference to the provision "Significant risks and challenges can arise if an institution decides to terminate a contractual agreement with a CSP without having previously established a comprehensive exit plan on the basis of a principle-based exit strategy", clarification is needed with respect to the meaning of "principle-based".	Requirements should be clearer.	ECIIA	Publish
38	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12	Amendment	"Other changes that could also lead to such a reason for termination include [...] (vii) continuous failure to achieve agreed service levels or a substantial loss of service, and (ix) a failure to successfully execute cloud provider test migrations at the agreed times". The last two points are not classifiable as "changes" but they are specific condition. We deem necessary to separate them from the previous termination reasons. More apropriate would be "Other reasons for termination include (i)….."	Suggestion to be clearer.	ECIIA	Publish
39	2.4 Exit strategy and termination rights 2.4.3 Granularity of exit plans	2.4.3	13	Amendment	"to any deterioration" is too expansive and should be replaced by "major/significant"	We suggest to narrow the scope.	ECIIA	Publish
40	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	2.4.4	14	Deletion	The paragraph 2.4.4 collapses Business Continuity and Exit Strategy considerations and introduces the concept of an "exit under stress or an exit without the cooperation of the CSP(s)". We believe this requirement is quite impossibile to be respected, a recovery for continuity purposes should happen in hours while an exit takes months. The only way this could be achieved would be to develop, matain and keep at scale different parallel systems performing the same functions using different architectures and infrastructure, that would mean to double costs and maintenance effort."	Impossible to comply with the requirements.	ECIIA	Publish
41	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5	14	Clarification	It is necessary to have a definition of 1st/2nd LoD responibilities on oversight/monitoring.	We recommend to clarify the responsibilities for each line (based on 3 lines model)	ECIIA	Publish
42	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5	14	Clarification	Further clarification and best practices are needed on how to „solve“ the CSPs „auditing support“ issue. This is a general problem - individual internal audit function cannot solve it.	We recommend best practices to solve the issue	ECIIA	Publish

43	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5	15	Clarification	The sentence "An institution's internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts)." should specify if it is a bout residual or inherent risk.	Need for clarification.	ECIIA	Publish
44	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5	15	Supportive/ Amendment	Last sentence of 2.5: We acknowledge that the practice outlined is good and aligns with best practices in audit procedures provided with the pooled audit approach of the Collaborative Cloud Audit Group. By requiring individual institutions to follow up directly with the Cloud Service Provider (CSP) on specific issues identified during a pooled / joint audit that are relevant only to that institution, it facilitates a focused, tailored and effective dialogue between the institution and the CSP to address any unique concerns or issues identified during the audit. regarding the rotation, we suggest "regular basis" rather	Element fully aligned with best practices, but it is difficult to systematically rotate the IA team.	ECIIA	Publish
45	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5.1	16	Clarification	Clarification needed in "In order to ensure an adequate level of quality, the institution should monitor the cloud services provided by the CSP. Relying solely on monitoring tools provided by a CSP in order to assess performance might not be sufficient in the case of outsourcing of critical or important functions" about the CSP's performance that should be monitored independently.	Need for clarification.	ECIIA	Publish
46	2.5 Oversight, monitoring and internal audits 2.5.2 Incidents reports and contractual details	2,5,2	17	Best practices	Request for best practice on how to establish a process to ensure that more details are being shared by the CSP	Best practices would help fulfilling the requirements	ECIIA	Publish
47	2.5 Oversight, monitoring and internal audits 2.5.3 Contractual clauses	2,5,3	18	Amendment	The contractual clauses could also include periodical checkpoints for the utilization / capacity review of the services provided.	Suggestion to include clauses in the section;	ECIIA	Publish
48	2.5 Oversight, monitoring and internal audits 2.5.3 Contractual clauses	2,5,3	18	Amendment	The sentence : •Contracts should include details of how the cost of performing on-site audits is calculated, ideally including a breakdown and indica-ting the maximum cost" should be changed : "contracts should include details of hos the costs of performing audits is calculated"	Commercially, it will be difficult to fulfil the requirements, audit costs are on top of the rest.	ECIIA	Publish