afme/
Finance for Europe

Association for Financial Markets in Europe

ECB Guide on outsourcing cloud services to cloud service providers

ID	Chapter	Detailed comment	Concise statement as to why your comment should be taken on board
1	**1. Introduction** **1.1. Purpose**	The Guide introduces prescriptive and granular expectations that 'gold plate' existing requirements on outsourcing, cloud and ICT risk management that will have potential contractual, operational and commercial impacts for FIs, as well as potential impacts to the resilience and competitiveness of EU financial markets more broadly. The Guide should not prescribe specific technology solutions and methodologies to address tech-specific risks that could easily become outdated. Specific technology solutions have downstream impacts on the technology stacks of financial entities that reduces the ability of entities to build stacks that are appropriate for their infrastructure. The Guide should provide flexible guidance that allows FIs to adapt risk management frameworks to cloud-specific risks. With financial entities under severe pressure to ensure DORA requirements are met by Jan 2025, as they also await crucial additional guidance in technical standards yet to be finalized, the Guide's prescriptive and expansive expectations add further complexity - rather than clarity - to the already challenging implementation of DORA. The current landscape includes a number of overlapping and often conflicting regulatory expectations (including the EBA Outsourcing Guidelines which the Guide references, however which industry anticipates will soon be updated to align with DORA).	The Guide's prescriptive and expansive requirements add significant complexity for FIs compliance with existing regulatory expectations, including DORA. The ECB should seek to amend specific technology solutions (e.g. containerization) from the Guide and remove wording that enforces specific measures. Further, given the timeline to DORA's implementation deadline, the ECB should align the timing of its guidance with DORA in a clear and pragmatic way. The ECB should be clear in the Guide regarding how they will utilize their expectations in supervisory interactions through the enforcement of DORA.

2	1. Introduction 1.2 Scope and Effect	***For the purposes of this Guide*** , it should be confirmed that critical and important functions ***within scope*** should be limited to only those functions from which systemic impacts may arise, in line with the ECB's definition reported in the section "Definitions of terms for the purposes of this Guide". This must be clearly and visibly stressed throughout the Guidance to avoid confusion with the wider definition of Critical and Important Functions under DORA. With the exception of CIFs, the ECB should adopt and ensure consistency with DORA terminology, for example, the definition of ICT asset should align with that set out within DORA.	Without the systemic lens, a number of proposals within the Guide would not be feasible. Where the ECB decides to use established terminologies it should align with DORA to avoid inconsistent regulatory approach.
3	1. Introduction 1.2 Scope and Effect	The Guide states that firms should take proportionality into scope but does not reference the rigorous proportionality principle embedded in DORA or the EBA Guideline. Proportionality references within the chapters are also applied randomly within individual chapters. For instance, the Guide applies requirements to services supporting CIFs in some cases, but not others. Additionally, it does not reflect the varying levels of risk or technical feasibility relevant to different types of cloud services (i.e. IaaS, PaaS and SaaS). Similarly, the Guide fails to apply materiality to supply chain scope. Without a clear and risk-based approach to the application of supervisory expectations to subcontractors, this could capture an unnecessarily broad scope of subcontractors. Given the Guide is intended to inform the ECB's expectations of DORA compliance, it should apply a materiality threshold that is consistent with DORA and what is ultimately applied in the final draft regulatory technical standard on subcontracting (i.e. subcontractors which "effectively underpin" CIFs).	The Guide should ensure a consistent application of proportionate and risk-based principles in alignment with DORA. Without this consistency, supervisory expectations could be interpreted as applying to a very expansive scope of cloud services and their subcontractors and will be overly burdensome to comply with. The Guide should apply an appropriate materiality threshold to risk management and supply chain scope that is aligned with DORA / the regulatory technical standard on subcontracting to uphold a risk-based approach that is feasible and addresses material risks.

4	1. Introduction 1.2 Scope and Effect	The ECB propose that where a non-CSP TPP is reliant on cloud services provided by a CSP the same supervisory expectations apply. This does not appear to consider the materiality or criticality of the services provided by the TPP, or define what is meant by "reliant" in this instance. The EBA's draft Technical Standards on the subcontracting of Critical or Important Functions limits its scope to those subcontractors which provide an ICT service which support critical or important functions, or material parts thereof. Furthermore, we understand that the EBA is considering specifying that these requirements would only apply to those subcontractors which "effectively underpin" ICT service supporting critical or important functions or material parts thereof, in line with its draft ITS on the Register of Information. Requiring firms to assess ALL of their Third-Party Providers, regardless of materiality, criticality or risk, to determine the degree of their reliance on CSPs would represent an extraordinarily disproportionate operational burden which could materially impact the commercial viability of institutions at a time when the ECB has been vocal about the need for banks to have sustainable business models. Furthermore, the ECB has failed to explain how these requirements should be applied to TPPs which are reliant on CSPs. Given that the population of institutions' TPPs which are reliant on CSPs is likely to be substantially greater than the number of services provided by CSPs, the ECB should clearly explain how each expectation should be delivered for both CSPs and TPPs. We would propose that the ECB remove this extension of scope and limit their expectations to institutions' use of cloud services provided by CSPs, and rely on the EBA's expected Technical Standards on the subcontracting of Critical or Important Functions to set out robust standards for the management of risks associated with subcontracting.	The existing planned scope does not consider proportionality, materiality or criticality, and will introduce substantial cost for EU institutions with no clear rationale as to the associated benefits from an operational or risk management perspective. Furthermore these requirements overlap (and conflict with) the Technical Standards on the subcontracting of Critical or Important Functions being developed by the ESAs.
5	1. Introduction 1.2 Scope and Effect	There is inconsistency in terms of the types of cloud services within scope of the guidance, and parts within. For example, whether this relates to cloud services supporting CIFs or all services, and which types of cloud service (IaaS/SaaS/ PaaS) are subject to specific requirements.	Without clarity that this relates to cloud services supporting CIFs, the guidance will be lacking in proportionality and feasibility. Additionally, without clarification as to the type of cloud service subject to specific requirements, there are certain expectations which are not even practically possible.
6	1. Introduction 1.2 Scope and Effect	The ECB does not indicate the timeline for its planned application of these expectations. As many of the proposed expectations go beyond the requirements of DORA, and institutions' implementation programmes are already well advanced, it would be helpful for the ECB to allow sufficient time for firms to implement their expectations following the completion of implementation of the legal requirements under DORA.	Changing the expectations for firms' implementation of requirements in relation to DORA at this late stage could endanger institutions' implementation requirements. An overly short implementation period could create significant operational risks, and harm firms' resilience.

7	1. Introduction 1.2 Scope and Effect	It is not always clear with who the obligation sits, whether a CSP or the financial entity.	Unless the CSP is the target of certain provisions, the proposed approach for example on joint testing, is unlikely to work in practice. This is especially the case with regards to Spot Checks, where a CSP is unlikely to be able to permit an FE to conduct spot checks in a multi-tenanted environment.
8	1. Introduction 1.2 Scope and Effect	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. This could cause uncertainty for financial entities regarding the application of NIS2 to the financial sector. There exist DORA equivalent requirements to the references to NIS2, which creates confusion due to the ECB's choice to reference NIS2 requirements over DORA.
9	1. Introduction 1.2 Scope and Effect	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" to avoid uncertainty in the definitions.	To avoid misinterpretation and ambiguity.
10	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	The ECB includes a requirement to for institutions to "ensure that the CSP has itself properly implemented the relevant checks", however it does not clearly establish what is means by "relevant checks". It would be helpful for the ECB to more clearly explain the scope and nature of the checks that CSPs should be expected to perform.	Lack of clarity regarding the ECB's expectations could lead to inconsistent implementation, and introduce an unlevel playing field.

11	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question	The final sentence on ensuring that CSPs have equivalent risk management practices, could lead to misunderstanding that CSPs have to mirror the obligations on FEs. This expectation goes beyond current regulatory expectations and reasonable risk management practices. The sentence should be deleted given the repetition with the preceding one, or at least it should be clarified that this is about assessing that "CSPs have established equivalently effective risk management practices."	The legal obligation for a CSP should be on assessing the FE can meet its regulatory requirements; not mirroring the FE obligations. It is not reasonable to assume that an FE can enforce their own risk management practices onto a CSP.
12	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	The risk considerations are prescriptive, expand existing requirements in DORA and EBA and do not reflect a risk-based approach. Additionally, some of the considerations are subjective, lack clarity, and also are not appropriate to be assessed at the pre-contractual phase, in particular 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", □consider "the risk of a significant increase in price"	There is a lack of feasibility and clarity regarding the ECB's expectations on pre-outsourcing analysis. . A number of the risk considerations are not appropriate to be addressed at the pre-contractual phase. The Guide should expressly apply a risk-based approach to the pre-outsourcing analysis.
13	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	Section states, "perform thorough analysis of control processes that will be established" - it is unclear if this is referring to controls that are to be established by the FI or CSP? If the latter, the concern is that FIs would be dictating to CSPs what their controls should be.	Lack of clarity.

14	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	It is unclear if financial service firms are being asked to audit the cloud providers individually. Would there be the option to have industry-wide joint pooled audits of CSPs? If this is an option, it would be beneficial to understand roles and responsibilities as well as ownership of action items.	Lack of clarity.
15	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	It should be added that institutions should perform analysis of the control processes "on the basis of the data flows provided". Proposed new wording: perform thorough analysis of the control processes that will be established on the basis of the dataflows provided.	In order to boost the feasibility of the guidance.
16	Chapter 2.1 Governance of Cloud Services 2.1.3. Consistency between an institution's cloud strategy and its overall strategy	There seems to be a broadening of the DORA strategy on 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 risk as stated in DORA.	The guidance is extending beyond DORA obligations and creating misalignment.

18	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	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 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 transfer 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 resourced firms which could afford to maintain this setup. An alternative approach being considered by many firms is logical segregation of backups within the same cloud provider. Recent incidents such as the UniSuper outage demonstrate that, even under the most extreme scenarios, provided the firm has a well-architected recovery capability, logically segregated data can be vital to recovery. We would propose that instead of prohibiting the use of the same CSP for backups, the ECB should instead require institutions to assess the resilience of their backups based on the risk associated with the services provided, including for instance the storage of back-ups in different cloud regions, use of active / active backups, multi-cloud strategies, secondary back-ups outside of the primary cloud etc. This should be in line with the measures considered within section 2.2.2 Proportionate requirements for critical functions.	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.

19	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	The ECB interprets Article 12 of DORA to require institutions to include back-ups for all CSPs. However, DORA Article 12 requires financial entities to develop and document policies and procedures specifying the scope of data that is subject to backup, and the minimum frequency of the backup, based on the criticality of information or confidentiality level of the data. The ECB's interpretation does not account for the legislative provision that this should be based on the criticality and confidentiality of the data stored. We would propose that the ECB amend this provision to explicitly recognise that institutions should determine the backup requirements based on an assessment of these factors.	Failure to consider the criticality and confidentiality of the data in question would go against the specific provisions of the DORA legislation itself. Furthermore, it would not align with basic risk management principles that the design and implementation of risk mitigants should be aligned with the risk which they seek to address
20	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	The ECB does not define a 'critical or important system' – this could be interpreted to be any system which in any way supports a critical or important function, which would not consider materiality. The ESAs' technical standards on the use of ICT services to support critical or important functions includes a risk assessment of the service provided by a TPP (which would include CSPs) to inform the degree of application of the requirements, including the potential impact of disruptions on the continuity and availability of the financial entity's activities. We would propose that the ECB's requirements for the use of CSPs to support critical or important functions be based on an assessment of the risks associated with those services, rather than be applied across all CSP services regardless of the risks associated with them.	Failure to define what is meant by a 'critical or important system' would lead to inconsistent implementation, and could create an un-level playing field. These requirements should consider proportionality to ensure that risk mitigants are appropriate to the risk being addressed.
21	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	There seems to be some ambiguity about whether backup is required for data only or for systems (which is completely different in terms of impact technical feasibility or ability to be utilized in a resilience scenario). 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.	The ECB should provide clarification that backups should only be considered in relation to data storage-only. This represents an appropriate resilience strategy that can be utilized (within the same CSP) whereas a system backup would constitute a vast level of infrastructure and application build. A system backup in another CSP would not allow for equivalent services to be provided and could only be realised in weeks due to the technical difficulties involved.

22	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	The proposed worst case scenario of an entire CSP being not available and not cooperative is lacking in plausibility. Ultimately, this would require having it duplicated in a data centre. The only way this could be achieved would be to develop, maintain 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. It also does not consider the resilience measures in place within individual CSPs which would prevent such a failure from happening in the first place, or allow rapid recovery from such a failure. In the absence of a clear rationale of how such a failure could occur without mitigation by CSPs' own resilience measure, presumption of this degree of failure does not appear in line with the 'severe but plausible' basis of most stress scenarios. Furthermore, a CSP being unavailable would apply to all commercial and individual users of the CSP and would constitute a significant economic and political event with severe financial stability implications for the global economy. We instead believe that BCM measures should address severe but plausible scenarios impacting the cloud services which they leverage, which would consider the mitigations which can be deployed by the CSPs themselves in plausible scenarios.	The Guide's reference to bankruptcy, alongside a lack of CSP cooperation or involvement, is unlikely to occur in reality and would reflect a scenario whereby the wider European and global economy would be affected. AFME recommends that the ECB changes the scenario and focuses supervisory expectations on severe but plausible scenarios, while considering worst-case scenarios with more realistic assumptions.

23	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	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 to the CSP. Given the tools used may be proprietary, this often will 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 premise in this example would require conversion and significant testing rendering the strategy ineffective for limiting disruption to within agreed tolerance levels. From a resource perspective, maintaining these compute capabilities would not be feasible save for perhaps the very largest financial entities. Even then, it would be cost prohibitive 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 financial entities and would effectively erode the value add 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 ability to bring data and applications back on-premises"	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.

24	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	Given the ESAs' development of technical standards covering Article 6, it seems unusual that the ECB would separately develop its own interpretations of Article 6(8) which go beyond the standards developed by the ESAs in their mandate under DORA, and which could be interpreted as the ECB seeking to take on a regulatory role rather than a supervisory role. Regarding the ECB's interpretation of Article 6(8) in particular, DORA requires (which is expanded upon in the ESAs' technical standards) that institutions develop an operational resilience strategy, and sets the components explaining how it will deliver against its operational resilience goals. It does not require institutions to consider specific resilience measures. Furthermore, the specification of specific resilience measures risks the guidance quickly becoming out of date. We would propose that the ECB amend section 2.2.2 to remove the reference to specific resilience measures. If not, applying these measures to SaaS and PaaS cloud services may be particularly difficult to the extent of unfeasibility or have negative impacts. Therefore, we would suggest that the focus of these measures should be on IaaS, where institutions have more control over the underlying infrastructure.	The current drafting risks misalignment with the DORA requirements referenced, and excessively prescriptive requirements undermines the principle under DORA that institutions should determine the resilience measures most appropriate to their needs.
25	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	Maintaining multiple CSPs increases operational and cybersecurity risk. Operationally, multi-cloud options require multi-lingual internal teams and a greater risk of complexity due to differing control places alongside on-premises infrastructure. Cybersecurity risk increases due to attack surfaces materially increasing, which adds further risks relating to oversight. These are all considerations that should be taken account of in any form of cloud adoption. It would also be prohibitively expensive. A multi-cloud live live cloud adoption is the most costly form of adoption and would materially increase the operational budgets of ECB-firms to maintain, thus likely creating a highly uncompetitive market in the EU.	A rigid interpretation of the measures described in 2.2.2 could result in a highly uncompetitive marketplace for ECB-supervised firms whereby they are enforced to maintain separate equivalent technology capability across multiple CSPs and on-premise infrastructure. This would render the adoption of cloud services as illogical and outside of budget capabilities. Amendments and greater proportionality should be applied in order to ensure a level-playing field and the ECB proposing realistic technology strategies.

26	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	Recommend deleting: *To this end, institutions 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. For example, institutions could consider developing mature virtual machine-based applications and/or containerising their applications in the cloud environment, or they could consider portability aspects of Platform as a Service solutions*	This level of prescription will ensure that the guidance quickly becomes out-of-date as practices and technologies rapidly evolve in this space. This occurred with the 2013 MAS Risk Management Regulations. Additionally, the enforcement of a particular technology solution, such as containerizing, has downstream impacts on the technology stack that will be produced by the financial entity. The ECB should avoid prescribing specific forms of technology that will reduce the options available to developers when building their tech stacks.
27	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	The ECB's interpretation of Article 28(8) go beyond the requirements envisioned in the primary legislation, as well as conflicting with the technical standards developed by the ESAs on the use of ICT services supporting Critical or Important functions. In particular, Article 10 of these technical standards states that, "the financial entity shall ensure that the exit plan is realistic, feasible, based on plausible scenarios and reasonable assumptions and shall have a planned implementation schedule compatible with the exit and termination terms established in the relevant contractual arrangements". Both the primary text and the technical standards seek to ensure that exit strategies address plausible scenarios and reasonable assumptions in relation to the services being leveraged. The ECB's expectation that institutions be able to remain fully operational in circumstances explicitly outside of the exit plans appears to go beyond these requirements. Furthermore, the ECB's specification of these requirements in relation to "Critical Functions", which they define by referring to the definition of "Critical or Important Functions" per the EBA's guidelines on outsourcing, which is not aligned to the definition of "Critical or Important Functions" under DORA does not appear in line with the scope of Article 28(8) in DORA, which is applied to ICT services supporting Critical or Important Functions (using the DORA definition).	Misalignment between the ECB's expectations and the DORA regulation / supplementary technical standards could lead to confusion for institutions, inconsistent implementation and an unlevel playing field.

28	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	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.	To avoid misinterpretation and ambiguity
29	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	Right to audit notice clauses (e.g. 30 days notice) may impact ability to conduct spot checks at short notice in order to assess CSP readiness. We suggest rewording 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 should perform, ***whenever possible,*** spot checks and/or tests at short notice in order to assess its readiness for an actual disaster event."	Lacking in proportionality
30	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	Spot checks on all cloud services as part of disaster recovery tests would not be possible. Without proportionality, this would constitute spot tests across all IaaS, PaaS and SaaS individual services that a financial entity utilises, which can be hundreds of services. Equally, DORA introduces a significantly expanded testing regime for financial institutions and their third parties, including threat-led penetration testing. The Guide gold-plates with the addition of 'spot checks' while not recognising that these forms of test will have to be agreed by the relevant CSP. Similarly, not relying on disaster recovery certifications should be limited to IaaS.	Spot checks significantly expands beyond pre-existing DORA testing requirements, are unrealistic and could be operationally burdensome when applied to all cloud services.

31	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	The suggestion that contracts with CSPs should be remediated as part of the ECB guidance should be deleted. 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. Additionally the non-binding nature of the guidance means that CSPs are likely to push back on additional contractual remediation and the Guidance should recognise these practical difficulties. These difficulties will be exacerbated when applied to non-CSP third-party provider (TPP) reliant on cloud services provided by a 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 the contract remediation efforts as part of DORA, which already represent a significant operational uplift for financial entities.
32	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	With regard to the shared responsibility model, clarification is needed on whether the DRP is related to CSP infrastructure or to Institution's configurable services running on cloud environment.	To avoid misinterpretation and ambiguity
33	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	The concentration assessment provisions, which we undertstand to be at the entity level, fail to take account of the assessments to be undertaken by authorities as part of the incoming Critical ICT Third Party Provider regime and other DORA Level 2 technical standards, some of which are still to be finalised. These should be leveraged, rather than expecting assessments on a regular basis by the firm. The preliminary assessment of ICT concentration risk oblligated by Article 29 DORA is the key.	The guidance should be embedded in the wider regulatory landscape.

34	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	Article 9 of DORA requires firms to use ICT solutions and processes to address risks in relation to data security, integrity, availability and access. While we agree with the ECB that institutions need to protect their data, we would note that DORA does not set specific requirements for the encryption of data, and that this is likely intentional. Furthermore, the ESAs' final technical standards on the ICT Risk Management framework establish that institutions should have a policy on encryption and cryptographic controls, based on data classification and ICT risk assessments, and which should include rules for the encryption of data at rest, in transit and in use, where necessary. It specifically acknowledges that the encryption of data in use may not be possible, and that other measures may be used to protect data in use instead. IaaS providers, for instance, automatically de-crypt data if the individual has appropriate access levels, which makes encryption redundant. The ECB's interpretation fails to take into account firms' assessment of the ICT risks associated with the data, and its classification. There are significant technical limitations for the encryption of data at rest and in use, and our view is aligned with that of both DORA and the ESAs in that firms should select the data protection controls based on the data and risks in question, rather than be required to apply specific controls across all data.	Establishing specific requirements for data encryption across all data in cloud fails to consider the data classification and risk assessment for that data, and does not consider alternative methodologies and controls which may be employed to protect data.
35	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	Data tracing for compliance monitoring would be extremely difficult to implement, and disproportionate to the associated risks. A more appropriate measure would be for institutions to establish contractual restrictions on the locations which may be used to store the data, and to require CSPs to attest to their compliance with these requirements, potentially supported by inclusion of data location within the scope of audits where appropriate. We propose that this section be amended to allow firms to determine the most appropriate approach to monitor compliance of location restrictions for their data.	Current proposals are disproportionate, and will prove extremely technically challenging and costly as compared to alternative methodologies, and may not be as effective.
37	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	The requirements in this section appear duplicative with the data security measures covered under the technical standards developed by the ESAs as part of their mandate under DORA, in particular Articles 6 and 7. We would suggest that the ECB avoid duplication of requirements to reduce the risk of conflicting requirements and disconnect between the two sets of requirements should either be reviewed in the future.	Duplicative and conflicting requirements between the ECB's guide and the technical standards developed by the ESAs as part of their legal mandate under DORA, which have reviewed and adopted by the European Commission and the EU legislature, and subsequently published in the Official Journal of the EU could lead to confusion, inconsistency in implementation, and the introduction of an unlevel playing field.

38	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data	The recommendation should be a list of unacceptable countries based on the firm's risk management practices, rather than a list of acceptable countries. If the aim is to ensure that FIs are aware of data processing and storage requirements across jurisdictions, the ECB should not prescribe the method (e.g. list of acceptable or unacceptable countries) by which an FI does this. Additionally, subcontractors "relevant for" the cloud does not appropriately apply materiality and therefore risks 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 states that a financial entity must monitor a CSP''s access to their data. In a shared, multi-tenant environment, this would require a financial entity to actively monitor all hosted workloads despite workloads often constituting temporary storage. This is technically impossible and outside of the ability for a financial entity.	Monitoring of a CSP''s access to a hosted workload should be on a risk-based basis.
39	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data	As flagged above, regarding the use of subcontractors, this is a topic on which the ESAs are developing detailed requirements as part of their mandate under DORA, which will be subject to review and adoption by the European Commission and subsequent review by the co-legislators. More specifically, the ECB's proposals fail to take into account consideration of materiality, criticality or risk associated with these subcontractors. The assessment of all subcontractors across all CSPs would be extremely onerous and disproportionate to the risks associated with those subcontractors. While the final technical standards are still in development, the requirements in relation to subcontractors are limited to where the TPP provides ICT services supporting Critical or Important Functions (CIFs), and we understand that the ESAs intend to further specify their requirements to those subcontractors which materially underpin those CIFs. Consideration of risks is a fundamental element of risk management frameworks, and should be incorporated as appropriate for all measures. We would propose the deletion of requirements which overlap and potentially conflict with the final technical standards being developed by the ESAs.	We would encourage the ECB to avoid pre-empting these formal standards to reduce the risk of conflicting or overlapping requirements.

40	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	The inventory of all ICT assets appears at odds with the Cloud based scope of this guidance. Additionally, a definition of Outsourced Asset is required: the EBA Guidelines on outsourcing arrangements cover the outsourcing of "processes" or "functions". It is unclear what cloud service would constitute an asset, what would be considered different assets of the same kind or different types of assets, especially regarding the adoption of SaaS products or that of serverless services.	The scope of the guidance is cloud services, so there should be no broader obligation on other types of ICT assets.
41	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	The requirement for individual clauses should be deleted. 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 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 agreeing individual clauses with the CSP when entering into a cloud outsourcing arrangement 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.
42	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements	The Guide should specify that this expectation "the institution should, as a minimum, look at how the structure provided by the CSP for the cloud services fits with the institution's roles and responsibilities to ensure the effective segregation of duties" is only focused on Identity and access management (IAM)	Clarification on perimeter of roles and responsibilities regarding IAM

43	2.4 Exit strategy and termination rights 2.4.1 Termination rights	The Guidance creates new additional termination rights which go beyond existing regulatory expectations and commercial practice and do not apply proportionality and risk-based principles. It would also be unreasonable for many of these to be detailed in the contractual arrangements with CSPs for example around an excessive increase in expenses. Additionally, the Guide incorporates grounds that are covered by Article 28 of DORA, but uses different terminologies. This adds unnecessary confusion and complexity to industry's understanding and application of DORA. The first two paragraphs of paragraph 2.4.1 should be deleted. In the event they are not, the reference in any changes in cybersecurity obligations being cause for termination should be exchanged with violations to cybersecurity obligations. Regarding the ECB's expectation that it should be possible to terminate only some of the services provided by a CSP, this is likely to be extremely difficult in practice. Many services provided by CSPs are highly intertwined and difficult to legally separate. We would welcome the ECB's recognition that this would be beneficial where feasible, and acknowledgement that it may not be possible in the majority of cases.	Seeking to create non-binding termination rights which do not reflect existing legal or market practice is lacking both proportionality and feasibility. This goes beyond DORA and EBA requirements. Additionally there are other ways in which to tackle the underlying risks and provide comfort to regulators, without the need to resort to termination.For example additional safeguards on risk management, including through the incoming CTPP regime
44	2.4 Exit strategy and termination rights 2.4.1 Termination rights	Regarding the ECB's proposals that "institutions should ensure that all suppliers of subcontracted services supporting the CSP comply with the same contractual obligations that apply between the institution and the CSP". This overlaps significantly with the technical standards being developed by the ESAs in their mandate under DORA on the subcontracting of critical or important functions. However, the ECB does not consider either the criticality of the service being provided by the CSP or the materiality of the services being provided to the CSP by its subcontractors. This creates an extension of scope which will capture fourth party providers who do not have any material impact on an FE's abilities to provide its services, for instance an institution's catering supplier which uses cloud services for scheduling.	This consideration of criticality and materiality is fundamental to the principles of risk management, as many services provided by CSPs may not be critical to the functioning of the institution, and many of their subcontractors may not have a material impact on the CSP's ability to provide those services (e.g. catering suppliers).
45	2.4 Exit strategy and termination rights 2.4.1 Termination rights	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"	To avoid misinterpretation and ambiguity

47	2.4 Exit strategy and termination rights 2.4.2 Components of the exit strategy and alignment with the exit plan	This creates a subject matter expert dependency. To rebuild a service, and FE would need to have immediate access to SMEs who will be able to rebuild in a timely manner, or be allowed a feasible timeline to identify the right contact.	Lack of feasibility.
48	2.4 Exit strategy and termination rights 2.4.3 Granularity of exit plans	The execution of exit plans is by nature an exceptional activity, and so often requires additional resources and capacity beyond those required for BAU activities. As such many exit plans involve the hiring of professional services and / or contractors to augment the institutions' normal staff. The ECB's proposed requirement for institutions to check that they have the personnel required for their exit plans could be interpreted to require institutions to maintain sufficient staff to execute against exit plans on a full-time basis, which would be an egregious additional cost beyond what is required for BAU activities. We would propose that the ECB amend this section to read: *Institutions should check that they have the personnel required for their exit plans, or a plan for the additional staff which would be required and, by conducting a walkthrough of the tasks involved, ensure that the planned staff available ~~are~~ would be able to perform the proposed tasks outlined in the exit plan.*	Potential lack of feasibility.
51	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	The Guide does not apply an explicitly proportionate and risk-based approach to exit requirements by failing to limit expectations to services supporting CIFs to ensure the feasibility of the guidance.	The Guide should reflect proportionate and risk-based principles in existing guidance by applying exit requirements to services supporting CIFs.
52	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress	The reference to conflicting legislation appears to be referencing potential third country sanctions. This should be dealt with separately.	The guidance should remain technical in nature, rather than incorporating political discussions best reserved for other policy vehicles.
53	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	The wording currently refers to all ICT risk management requirements, rather than those relating to Cloud. Independent monitoring should also be limited to cases in which the institution has reason to believe manipulation can occur.	Extension of scope in the guidance beyond Cloud and lack of proportionality.

54	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	The document states, “It is good practice for institutions to work together to audit a CSP, putting together a joint inspection team containing at least one technical expert from each institution”, however, Financial service firms may not have the authority to force CSPs to submit to this. The section should clarify how scopes would be defined for a joint audit when firms may be utilizing different service offerings provided by a CSP with various levels of criticality. Additionally, FIs may not want to disclose to other firms in the pool the specific capabilities that they are using.	In light of separate guidance being produced on pooled auditing this guidance should refrain from overlap.
55	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	The guidance should suggest what other tools should be taken into account if the ECB is to state that monitoring tools provided by a CSP might not be sufficient. We would suggest that independent monitoring tools can be replaced by relying on CSP tools if they are reviewed periodically in a risk-based approach to ensure their adequacy.	Lack of clarity about ECB expectations without further examples.
56	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	We would propose that the ECB amend its proposed requirements that institutions’ oversight functions should be able to follow up in detail on “any incident that occurs at the CSP” to account for impact on the institution in question. CSPs offer a large number of services to a variety of institutions, including non-financial institutions. CSPs would not be able to share details of incidents which are not relevant to a give institution, given confidentiality constraints. Furthermore, institutions would not wish to have access to such information. We would propose that this statement be amended to read: *The institution’s oversight function should be able to follow up in detail on any incident impacting the institution that occurs at the CSP.*	The lack of any link to an impact on the firm would lead to overreporting of incidents, which carry no potential systemic impact.
57	Box 2: Contractual clauses	We propose the call for SCCs is dropped given that there is a EU forum already reviewing the issue, and it has not yet produced any standardised clauses given variations in industry practice and outlook. 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.
58	Box 2: Contractual clauses	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.

59	Box 2: Contractual clauses	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.