EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
Banking and Payment Federation Ireland

Contact person

Mr

First name
Peter

Surname
McGuigan

Email address
peter.mcguigan@bpfi.ie

Telephone number
+32 470 60 46 53

☐ 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 1.2 Scope and Effect	1	3	Amendment	In our view, the draft Guide does not reflect the DORA proportionality principle that considers the nature of the engagement or dependency on a financial entity's services or activities. Effective and proportionate risk management should take into account the cloud service and not be applied on a blanket basis across all SaaS, PaaS and IaaS solutions. We therefore recommend that the ECB Guide recognises the DORA proportionality principle or refers to the criticality of the cloud services on a financial entity's services or activities. We would therefore make the following drafting recommendation: 1.2: "When applying these expectations, account should be taken of the principle of proportionality as reflected in Article 28(1)(b) of DORA."	Having an ECB guide can often be useful in terms of providing supervisory expectations to firms, like industry has seen in other areas. It would, however, be useful if the ECB could further elaborate and contextualise the rationale for producing a guide on the use of a specific technology, like cloud services, given the substantial overlap of the draft guide with the technical standards under development by the ESAs as part of their mandate under DORA. In particular, we would highlight that the ESAs specifically outlined that it would did not include any cloud computing issues in its final draft RTS on the ICT Risk Management Framework stating the following: "The inclusion of cloud computing specific aspects was controversial, and it was chosen not to introduce any technology specific requirement based on the principle of technological neutrality, and to identify requirements related to ICT assets or services provided by ICT third party service providers in general. The ESAs may consider developing further guidelines in the areas that have been removed from the RTS, being those very important, and also on cloud computing security aspects". By taking the decision to develop this Guide it would appear to go against the ESAs' determination that cloud-specific requirements would breach the technology neutrality principle and pre-empts potential further work by the ESAs on cloud computing security. Alongside this, we believe that the Guide does not include a sufficiently detailed proportionality principle that reflects the intent of the Digital Operational Resilience Act (DORA) or the different types, or materiality, of outsourced cloud services. The EU regulatory landscape already consists of a number of overlapping rules and guidance that cover general outsourcing, cloud outsourcing and ICT security risk management which currently sit alongside DORA's harmonized and comprehensive framework. Whilst the ECB's Guide is intended to give clarity to the ECB's expectations on DORA compliance – which in itself can be positive – the current drafting seems to add further prescriptive guidance that expands DORA's scope and requirements and adds another layer of overlapping guidance for ECB-supervised entities to comply with. We would, therefore, urge the ECB to revise the Guide to ensure a more flexible and risk-based guidance, rather than prescriptive expectations, that will allow financial institutions to adapt their risk-management frameworks to any cloud-specific or evolving technology risks.	McGuigan, Peter	Publish
2	1. Introduction 1.1. Purpose	definitions	2	Amendment	We believe that the Guide creates interpretation issues by inconsistently applying expectations for outsourced cloud services that support Critical or Important Functions (CIFs) in certain chapters and not in others. For example, criticality is referenced in relation to cloud resiliency, assessment of concentration risk, access management, exit plans and independent monitoring, but not disaster recovery strategy, ICT security and location of data. As a consequence, we believe this approach would be disproportionate and add complexity to the framework. For instance, applying disaster recovery 'spot check' requirements across every SaaS provided by a firm would be disproportionate and overly burdensome to achieve. As cloud technologies cover a significant array of outsourced activities, this would constitute a vast level of operational change with limited benefit nor recognition of effective risk management practices. We recommend that the ECB includes a more detailed proportionality principle that applies to all Chapters or is more specific concerning their expectation for cloud outsourcing as it relates to CIFs. Furthermore, the terminology and definitions around criticality is itself inconsistent and could result in firms taking vastly different approaches to implementation of the guide and DORA, ultimately hampering harmonisation. Specifically, the draft guidance uses two definitions regarding the criticality of functions supported by CSPs, "critical or important functions", and "critical functions". "Critical or important functions" is defined on page 2 in the definitions table under section 1.1 with a definition which appears derived from (but not identical to) the definition of "Critical Functions" from BRRD rather than the more recent definition of a "Critical or important function" under DORA. Under section 2.2.2 Proportionate requirements for critical functions the ECB then use the term "Critical Functions", which they note is as defined in paragraph 29(a) of the EBA Guidelines on outsourcing arrangements. Paragraph 29(a) of the EBA's Guidelines on outsourcing arrangements defines the term "Critical or important functions" for the purposes of those guidelines.	The use of two different terms and definitions for the criticality of functions within a single guidance document may create confusion amongst in-scope firms, which will be further compounded by using a pre-existing definition of "Critical Functions" to define "Critical or important functions" while in parallel and conversely using a pre-existing definition of "Critical or important functions" to define "Critical functions", and neither of these definitions being aligned with the most recent (and arguably most high-profile) definition of the term "Critical or important function" under DORA. We would also note that we understand that the EBA expects to review its Guidelines on outsourcing arrangements in the near future, which may well involve aligning the definition for "Critical or important functions" with that used in DORA. We would encourage the ECB to use a single classification of the criticality of functions and this should remain consistent with DORA and be aligned with its definition. There is already a significant convergence across different regulations in the terminology and criteria used to identify what is 'critical'. Given the ECB's guide intends to reflect the ECB's expectations to understanding of DORA and how its requirements apply to the banks it supervises in the context of cloud outsourcing, having a definition aligned to DORA in the Guide would provide welcomed clarity and consistency to industry in meeting supervisory expectations.	McGuigan, Peter	Publish
3	1. Introduction 1.2 Scope and Effect	3	3	Amendment	We would highlight that the extension of the ECB's expectations to TPPs which are reliant on cloud services provided by a CSP fails to define what it means by "reliance", and does not consider either materiality or risk. 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 certain 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 any of the proposed 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 further elaborate how each expectation should be delivered for both CSPs and TPPs. We would, however, 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. At a minimum, we would recommend that the ECB defer further development of its expectations on cloud outsourcing until the Technical Standards on the subcontracting of CIFs is complete, to enable them to align their proposals with the EBA and avoid divergence.		McGuigan, Peter	Publish
4	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.2.2	7	Amendment	Based on the comments provided under para 3 of "introduction 1.2 scope and effect" we would recommend the following text be deleted: 2.2.2: "For example, institutions should 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." The Guide, furthermore, includes multiple references to the NIS2 Directive when informing the ECB's supervisory expectations, despite DORA being confirmed as lex specialis to NIS2, which will cause interpretation concerns for the sector. References are included in 2.2.1, 2.2.3, and 2.3 (business continuity measures, disaster recovery strategy, ICT security and risk management), and all refer to requirements in NIS2 that exist within DORA in a greater level of detail. DORA includes a Chapter (Chapter 6; Article 24-26) within the Risk Management Framework dedicated to business continuity plans and disaster recovery while the references to incident response and recovery are intrinsic to the RTS in its entirety. The Guide would be aligned to DORA if the CIF definition was made consistent and references to NIS2 were removed. Finally, there is no clear indication of the timeline over which the ECB expects the requirements set out in the guide to be delivered. As many of the requirements go beyond existing requirements (under DORA or otherwise) and industry practice, implementation will take a substantial amount of time. Given industry's ongoing work to achieve compliance with DORA, the introduction of new additional requirements at this late juncture could endanger institutions' implementation of DORA requirements, and could generate additional operational risks and harm institutions' resilience.		McGuigan, Peter	Publish

5	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis	2.1.2 bullet 3	4	Clarification	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.		McGuigan, Peter	Publish
6	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		4	Clarification	The risk-considerations are unnecessarily prescriptive, expands DORA's requirements without reflecting the risk-based approach taken in DORA and the EBA guidelines with respect to ex-ante risk assessments. The Guide should expressly state that financial entities should, on a risk-based approach, identify and assess all relevant risks …etc. Additionally, it would not be feasible to assess some of the risk considerations at the pre-contractual stage, while we would argue that the risk considerations described therein lack clarity or could be considered subjective – including: - 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 - the risk of a considerable fall in quality; - 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. - the risk of a significant increase in price; - not feasible at the pre-contractual stage. This risk is managed through contractual provisions.		McGuigan, Peter	Publish
7	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions	2.1.1	5-6	Clarification	The ECB's Guide prescribes particular forms of technology solutions to scenarios which may not be appropriate, risk-based or the most resilient solution depending on the ECB's scenario. Whereas 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 that this requires institutions to include back-ups for all CSPs. In our view, this does not account for the legislative provision that this should be based on the criticality and confidentiality of the data stored. We would therefore recommend that the Guide should consider what risks a financial entity may need to consider instead of prescribing a solution. Enforcing back-ups outside of the individual CSP that hosts services is a blanket requirement that could also be resolved with a multi-regional back-up, on premises back-up or a differing architecture of workloads to aid resilience or portability. The level of back-up required, in addition, is unclear and could infer a multi-cloud active deployment which is highly complex to maintain, the highest cost of any deployment (with significant colleague training increases) and subject to considerable cybersecurity risk due to the expansion of the attack surface. The Guide also says back-ups critical or important systems 'should not be stored in the cloud' which hosts the service rather than 'should not be stored with the same CSP'. Is it correct to understand that data backed up to a different cloud with the same provider (e.g. in a different data centre) would be acceptable? This seems to be the case but given the preceding sentences refer to failure of the service provider it would be good to confirm this in the final Guide. Separately, the ECB do 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. Additionally, there are many benefits to institutions of maintaining back-ups within the same cloud as the service provided, including speed of recovery and reduction of impacts with certain issues, as demonstrated by the recent UniSuper case. Furthermore, if the final Guide applies these requirements for all CSPs, we would propose that instead of prohibiting the use of the same cloud 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 ECB's expectations that institutions address a scenario in which all cloud services provided by multiple CSPs are not available concurrently if applied to all ECB-supervised financial entities, could not occur technically in a realistic scenario. ECB expectations should be predicated on scenarios that are more realistic. Furthermore, such a scenario 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. 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.		McGuigan, Peter	Publish
8	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2 (last bullet)	7	Amendment	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 seem to 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 appear to require institutions 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. The Guide's inclusion of various forms of cloud adoption for cloud resiliency do not reference the difference in operational and cybersecurity risk between each type of adoption. While the sector appreciates the inclusion of a risk-based approach for cloud adoption, the significant increases in complexity and trade-offs should be recognised by the ECB. For instance, a hybrid cloud architecture will introduce data transfer considerations and a reduction in a financial entity's end-to-end security visibility. The use of multiple CSPs to switch workloads introduces technical issues that can be unfeasible to implement across all of a CSP's services, as recognised by the EU's Data Act. These operational risk considerations have to be considered by a financial entity before determining their cloud adoption and should not be enforced via supervisory guidance. We therefore recommend that the risk-based approach stated by the ECB should also reflect the cloud resiliency option as well as the services or data represented. Between these two sets of consideration, we propose that section 2.2.2 be amended to read as below, without the bullet points which currently follow it. 2.2.2: "… the institution should assess the resilience requirements for cloud outsourcing services provided and the data managed and, following a risk-based approach **that takes into account the cloud adoption measure**, decide on the appropriate cloud resilience measures."		McGuigan, Peter	Publish
9	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions	2.2.2 (last bullet)	7	Amendment	The ECB's interpretation of purposes of Article 28(8) appears to 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). The Guide also includes enforcement measures that would result in a significant change to the technology stack of financial entities and would enforce a simplification of workloads supporting Critical or Important Functions. The ECB is clear that, for critical functions, a financial entity "must retain the ability to bring data and applications back on-premises." The SaaS, PaaS, or IaaS providers that could be supporting a critical function do not all provide critical services and, if they are non-operational, will not affect the service that is provider to the customer or the ICT system they are supporting. There are, in addition, significant technical complexities in architecting portability between CSPs and on-premise infrastructure, especially in relation to SaaS or PaaS. Continued innovation of services would have to be consistently updated within an entity's on-premises infrastructure and, in certain circumstances, could be beyond the capabilities of a financial entity's data centres. In this respect, it is not an appropriate risk management approach to mandate one specific cloud resilience option that does not reflect the cloud service being used. Multi-region capability, for instance, provides a significant degree of resilience and a financial entity could architect certain aspects of the service to be portable to their on-premise infrastructure, which can ensure the continuation of the service for the customer. Furthermore, the maintenance of on-premises infrastructure to enable the ability to bring data and applications back on-premises would directly and immediately counteract almost all of the commercial benefit to the use of cloud services. This would substantially harm the commercial viability of EU financial institutions, and could undermine the business model sustainability of firms. It is also likely to increase costs for EU customers, and inhibit institutions' abilities to provide financing and services to the real economy. This very specific requirement for financial entities to implement specific and extremely costly technology infrastructure does not appear to be grounded in either the primary DORA legislation, or the supplementary technical standards. We therefore recommend greater flexibility is applied and that the ECB does not enforce technology infrastructure requirements on financial entities via Supervisory Guidance. 2.2.2 "The institution **should** consider the ability to bring data and applications back on-premises **depending on the cloud service**."		McGuigan, Peter	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	2.2.3 (para 1)	7	Amendment	The Guide expands the testing requirements placed on ECB-supervised entities for their third-party providers. DORA already includes a material expansion for the testing requirements placed on financial entities, including testing backup procedures, ICT response and recovery plans, ICT tools and systems and more rigorous Threat-Led Penetration Testing that will apply to ECB supervised firms. The Guide in our view further expands this requirement to include spot checks on cloud providers to assess readiness for disaster events. It is unclear if this is achievable in reality and if CSPs would be able to continually allow spot tests across all ECB-supervised entities alongside shared TLPTs in their control environment. The addition of spot checks is disproportionate and unclear regarding its utility to demonstrate readiness for a disaster event. For instance, an industry table top exercise, or the validation of CSPs' plans via audit could provide greater levels of information. We recommend that the suggestion for spot checks is removed.		McGuigan, Peter	Publish
11	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 (last para)	8	Deletion	The ECB also states in the draft guide that a mechanism where a financial entity can secure remediation of deficiencies identified during testing is via a renegotiation of a contract with a CSP. The Guide should not encourage continual off-cycle contract renegotiations, which creates an undesirable legal environment without meaningfully addressing the deficiencies that have been identified and their potential solutions. Gaps identified should be addressed within the business continuity plan and the control environment of the CSP. We recommend this suggestion is removed.		McGuigan, Peter	Publish
12	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks	2.2.4	8	Amendment	In our view, the indicators are overly expansive, imposing additional risk management burden and lacking sufficient relevance to the assessment of concentration risk. Additionally, the Guide should expressly state that concentration risk should be assessed on a risk-based approach. The expectation to consider reliance by other entities is unreasonable and reflects sector-level concentration risk which is not feasible for a financial entity to take into consideration.		McGuigan, Peter	Publish
13	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 (opening para)	9	Amendment	Article 9 of DORA requires firms to use ICT solutions and processes to: (a) ensure the security of the means of transfer of data; (b) minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity; (c) prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data; (d) ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error. While we agree with the ECB that institutions need to protect their data, we would note that DORA very specifically does not set specific requirements for the encryption of data.Furthermore, the ESAs' final technical standards on the ICT Risk Management framework establish that institutions should have a policy on encryption and cryptographic controls, designed 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. 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. 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. 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. 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 monitoring of the location of a financial entity's data in a CSP via tracing is not possible in all circumstances. A financial entities data is stored in a CSP's multi-tenant environment whereby the entity, or any other individual or commercial actor, temporarily uses a particular instance that can constantly shift. No entity has the ability to monitor the entirety of a CSP's shared environment and this would constitute monitoring of all other providers that are utilizing that particular CSP. This would be overly burdensome and a disproportionate requirement that is outside of the capability of one financial entity. We recommend monitoring of the use of data is based on a risk-based approach where it is technically feasible to achieve, potentially supported by firms establishing 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		McGuigan, Peter	Publish
14	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	9-10	Clarification	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.		McGuigan, Peter	Publish
15	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data	2.3.2 (all paras)	10	Deletion	The Guide should not be prescriptive as to how financial entities manage location of data processing and storage risks including, for example, by drawing up a list of acceptable countries. Rather, it is common practice for firms to determine the locations in which their data can be stored or processed by their third parties. However, the creation of a list of "acceptable countries" is a crude method to approach this. Instead, institutions should assess the locations in which their data can be stored or processed on a case-by-case basis when entering into an agreement with a third party, based on the institution's assessment of the relevant risks and in line with applicable legal and regulatory requirements regarding the transfer of data (such as GDPR and Schrems), with any subsequent proposed change by that third party being subject to risk assessment and agreement by the institution. 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. We would encourage the ECB to avoid pre-empting these formal standards to reduce the risk of conflicting or overlapping requirements. 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.		McGuigan, Peter	Publish
16	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 (para 2)	11	Clarification	The Guide refers to "As part of this practice, an institution should, as a matter of best practice, maintain an up-to-date inventory of all the ICT assets it is responsible for under the policy, in order to ensure that all operational processes (monitoring, patching, incident management, change management, etc.) are extended to cover cloud assets." This would suggest given the definition provided in the document that an ICT asset consists of a software or hardware asset that is found in the business environment that there is an expectation that the institution includes CSP software and hardware assets supporting its services in its own ICT. Are we reading this correctly? This does not seem in line with the realities of how cloud resources work. In general, an institution contracts based on usage, not underlying infrastructure. The individual ICT assets, and indeed the total assets involved, will be highly dynamic. While it may be technically feasible to establish a dynamic tracking of which ICT assets are being used by a given institution at any time, the complexity and costs would be enormous, with no discernible benefits beyond the existing available information regarding firms agreed available capacity.		McGuigan, Peter	Publish

17	2.4 Exit strategy and termination rights 2.4.1 Termination rights	2.4.1	12-13	Amendment	The proposed guidance on grounds for termination of arrangements with CSPs significantly expand the scope of termination rights beyond what is currently established in DORA and the EBA GLs, and does not reflect proportionate and risk-based principles. It would be unreasonable to expect the reasons for termination detailed in the guide to be reflected in contractual arrangements with CSPs. The Guide therefore creates prescriptive, but non-exhaustive and non-binding expectations that go beyond acceptable legal and market practice. This would unnecessarily complicate the implementation of effective contracts and may prompt unnecessary off-cycle contractual remediation. Existing termination rights would achieve the same protective outcomes. In particular, we would like to draw attention to the following specific elements: - excessive increase in expenses – It is not clear on what basis the ECB consider "an excessive increase in expenses under the contractual arrangements that are attributable to the CSP" to be within the considerations included within DORA 28(7). Furthermore, it is unclear what relevance this could have to termination rights, as costs normally only change at the point of renewal. In such a circumstance if the commercial terms were not acceptable an institution would move to an alternative supplier from the end of the existing contract with no need to terminate it. We would urge the ECB to remove this element from the Guide. - the relocation of business units or data centres – In our view, this requirement is too granular and 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. As such, we would recommend its deletion. - changes to national legislation or regulations applicable to data location and processing – similarly, 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. We would therefore suggest the ECB does not include this in its final Guide. - significant changes to the management of cyber risk in the subcontracting chain – this is also covered by general termination rights related to subcontractors under EBA GLs and DORA and in our view, does not warrant inclusion. - failure to successfully execute cloud provider test migrations at agreed times – from our perspective this is criterion is too granular. It is also unclear what the material risk is here while material breach termination rights would achieve the same outcome. - Expectation that it should be possible to terminate only some services – From members feedback, they underline that this would be extremely difficult to do 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. - 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, the final draft of which is expected to be published for adoption by the Commission on the 17th of July. 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 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). Given the extension of scope of this guide to also cover those TPPs which are reliant on cloud this is even more important, for instance an institution's catering supplier which uses cloud services for scheduling is not likely to warrant the enormous investment of resources that would be required to fulfil these provisions and which could be more effectively deployed in relation to more critical suppliers. The technical standards being developed by the ESAs, as instructed by the European legislature as part of DORA, have limited the application of requirements regarding subcontractors to those that support Critical or Important Functions (CIFs) as defined in DORA. Furthermore, we understand that following engagement with industry, the technical standards being developed by the ESAs will focus on those subcontractors which effectively underpin the CIF. We would suggest that the ECB remove provisions which overlap with the technical standards being developed by the ESAs to avoid duplication and / or contradiction, especially as these requirements will become legal requirements following adoption by the Commission and publication in the Official Journal of the EU after scrutiny by the European Parliament. At a minimum, the ECB should recognise that the management of CSPs' relationships with their subcontractors remains the responsibility of the CSP, and that while institutions may stipulate in their contractual agreements with CSPs that their contractual agreements with their subcontractors must follow the same provisions, it is for the CSP to comply with those contractual arrangements. More broadly, we would argue that by focusing on addressing the underlying risk, rather than prescribe specific considerations, financial entities can maintain effective risk management while avoiding unnecessary complexity in their contractual arrangements with CSPs, which could be further reflected on by the ECB. For example, the requirement to ensure that the termination notice period set out in the contract should allow the institution to transfer or insource in accordance with the exit plan does not reflect risk management practices whereby the notice period for termination has little to do with the transition of services, which is usually done during a period post the effective date of the termination of services		McGuigan, Peter	Publish
18	2.4 Exit strategy and termination rights 2.4.2 Components of the exit strategy and alignment with the exit plan	2.4.2	13	Amendment	The Guide should explicitly state that requirements on exit plans are for services supporting CIFs (consistently with / as part of the exit strategy as referenced in paragraph 2.4). Granular exit plans do not necessarily provide a useful tool and could become quickly outdated or not be relevant for the scenario.		McGuigan, Peter	Publish
19	2.4 Exit strategy and termination rights 2.4.3 Granularity of exit plans	2.4.3 (para 1)	14	Amendment	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 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.		McGuigan, Peter	Publish
20	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5	14	Amendment	The proposed good practice of institutions conducting combined audits is likely to represent unacceptable levels of operational and information security risks for the institutions in question. An alternative approach would be for institutions to leverage vendors to conduct audits on behalf of groups of institutions, an approach which has proved successful in other jurisdictions. This would provide the benefits of conducting combined audits while ensuring that firms do not expose their data, systems and processes to competitor institutions.		McGuigan, Peter	Publish
21	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs	2.5.1 (para 1)	15	Amendment	The ECB should not enforce monitoring of CSPs to be undertaken by a single centralised function or a single department within a financial entity. 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 would make the following reccomendation: 2.5.1: "… supervised institutions should retain expertise in-house, ~~with a centralised function or department being recommended for the monitoring of CSPs.~~ The monitoring…"	The Guide's logic for enforcing independent monitoring of CSPs is that a CSP could manipulate the information that is provided to financial entities. Independent monitoring would still require data to be provided by the CSP in other to monitor their services. In this respect, this would still entail a reliance on the CSP's information and would not result in a reduction in the risk of manipulation. We recommend this requirement is removed and only required on a risk-based basis or ensured via effective oversight of the CSP by the financial entity. The Guide's prior suggestions regarding maintaining expertise in-house should more effectively achieve the Guide's objectives, so long as the requirement is not construed as suggesting that more in-house expertise is required at all times.	McGuigan, Peter	Publish
22	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	2.5.2	16	Amendment	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 any or all institutions, 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.		McGuigan, Peter	Publish
23	2.5 Oversight, monitoring and internal audits 2.5.2 Incident reports and contractual details	2.5.3 (bullet 3)	16	Amendment	It is not clear in the current draft of the Guide as to whether the contractual clauses covered are relevant specifically to standard contractual clauses, or if these should be considered to be best practices in general. The proposed best practice to include provisions covering the costs associated with on-site audits is not regarded as conclusively best practice in industry. Currently many vendors waive costs associated with audits, but requiring this to be covered in the contractual clauses could encourage CSPs to charge firms for audits. Additionally, the requirement to have providers sign a separate digital or physical copy may introduce operational difficulties which could be more easily addressed by the simple expedient of firms taking a copy of the terms at the point of signing, and requiring notice and non-objection to amendments to terms.		McGuigan, Peter	Publish