EUROPEAN CENTRAL BANK

BANKING SUPERVISION

# Template for comments

## ECB Guide on outsourcing cloud services to cloud service providers

**Institution/Company**

Futures Industry Association

### Contact person

**Mr/Ms**

**First name**

**Surname**

**Email address**

**Telephone number**

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

**General comments**

# Template for comments

## ECB Guide on outsourcing cloud services to cloud service providers

**Please enter all your feedback in this list.**
**When entering feedback, please make sure that:**
**- each comment deals with a single issue only;**
**- you indicate the relevant article/chapter/paragraph, where appropriate;**
**- you indicate whether your comment is a proposed amendment, clarification or deletion.**

| **Deadline:** | 15.07.2024 |
|---|---|

| ID | Chapter | Paragraph | Page | Type of comment | Detailed comment | Concise statement as to why your comment should be taken on board | Name of commenter | Personal data |
|---|---|---|---|---|---|---|---|---|
| 1 | 1. Introduction 1.1. Purpose | 1 | 2 | Amendment | The Guide introduces prescriptive requirements that significantly expand upon existing regulatory expectations in DORA and the EBA Outsourcing Guidelines. Particularly given the Guide has been issued at a time when industry is working to implement its compliance with DORA's requirements (and awaiting the finalisation of crucial technical standards), the Guide adds a further layer of complexity to existing overlapping regulatory expectations spanning outsourcing, third-party risk, ICT and cyber risk and risks undermining DORA's harmonization objectives.<br><br>In particular, we urge the ECB not to prescribe specific forms of technology solutions. A strict interpretation and application of the Guide could significantly impact cloud adoption, resilience and innovation in the EU financial sector. | The Guide should not prescribe specific expectations that add complexity to the implementation of DORA's requirements. Rather, it should provide flexible guidance focused on proportionate outcomes to allow FIs to tailor overarching risk management frameworks to the specific risk. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 1. Introduction 1.1. Purpose | 1 | 2 | Amendment | To facilitate the sector's implementation of DORA and the ECB's supervisory expectations, the Guide should align with DORA's scope and technical requirements.<br><br>In particular, the Guide should adopt DORA's definition of critical and important functions (CIFs) to support the sector in its understanding and implementation of the diversity in terminology used to identify "critical" functions. The Guide also separately references the EBA Outsourcing Guidelines in the context of "critical functions"<br><br>Similarly, we urge the ECB to adopt its terminology and scope with respect to subcontractors. The Guide references "suppliers of subcontracted services supporting the CSP" which is not used in DORA. The Guide should adopt the language in the draft ITS on the Register of Information (i.e. "subcontractors that effectively underpin the provision of ICT services supporting CIFs), to avoid further confusion and to ensure the appropriate application of materiality to supply chain scope. | Given the Guide is intended to inform supervised entities of its expectations of DORA compliance, it should align with DORA's scope and requirements. In particular, the definition of 'CIFs' and 'subcontractors effectively underpinning…etc" to ensure the appropriate application of a materiality to supply chains cope. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 3 | 1. Introduction 1.2 Scope and Effect | 1 | 3 | Amendment | Amendment Recommendation:<br>1.2: “When applying these expectations, account should be taken of the principle of proportionality as reflected in Article 28(1)(b) of DORA.”<br>The Guide does not take sufficiently into account the proportionality principle embedded in the Digital Operational Resilience Act (DORA) nor does it consider the various types and materiality of outsourced cloud services. The proportionality principle of DORA in relation to ICT Third Party Risk (Article 28) states that financial entities should take into account “the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities.” The ECB’s Guide does not reflect the DORA principle in regards of cloud services and therefore does not consider the cloud services relationship or dependency on the financial entity’s services or activities.<br><br>When managing third-party risk, it’s essential to consider the cloud service specifically rather than applying a one-size-fits-all approach across all SaaS, PaaS, and IaaS solutions. For instance, Microsoft have a SaaS data visualisation tool, called Power BI, which can support CIFs but, if non-functioning, would not result in any impact to the service provided to the customer or cause any financial impact. A more detailed proportionality principle would, furthermore, align to the EBA’s principle of proportionality whereby an institution should take into account “the complexity of the outsourced functions, the risks arising from the outsourcing arrangement, the criticality or importance of the outsourced function and the potential impact of the outsourcing on the continuity of their activities. We suggest that the ECB Guide acknowledge the proportionality principle outlined in DORA or consider the significance of cloud services for a financial entity's operations. | The Guide does not apply a robust and consistent approach to proportionate and risk-based principles that reflect and align with the approach taken in DORA and other related regulatory guidelines. The risk is that the Guide will apply to an overly broad scope of third-parties and cloud services, without reflecting the underlying risk and allowing FIs to take a proportionate approach to risk management based on nature of the cloud service and its potential impact to the delivery of services. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4 | 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 | 1 | 7 | Clarification | 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. It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity. For example, criticality is referenced in 2.2.2, 2.2.4, 2.3.4.2, 2.4 and 2.5.1 (cloud resiliency, assessment of concentration risk, access management, exit plans and independent monitoring respectively) but not in 2.2.3, 2.3 and 2.3.2 (disaster recovery strategy, ICT security and location of data respectively). This infers that a financial entity would be expected to perform “spot checks” across a wide range of disaster scenarios, encrypt all in transit and at rest data and forcibly locate data for all cloud outsourcing activities irrespective of materiality of the type of service. 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.<br><br>The Guide does not reflect the differing expectations of the ECB regarding different types of cloud services, such as SaaS, PaaS and IaaS. Differing types of cloud services have differing forms of resiliency controls, proprietary technology and roles within a financial entity’s technology stack. In a number of cases, the supervisory expectations of the ECB within chapters are clearly in relation to IaaS technology only. The EU’s Data Act, for instance, outlines clear instances where switching or interoperability between CSPs and on-premises are technically unfeasible and can constitute “significant interference in the data, digital assets or service architecture.” This, notably for cloud services which have a higher level of proprietary technology and therefore less substitutable services, should not be considered a supervisory expectation for all cloud services that a firm outsources. Further recognition of the variety of cloud services that exist should be included within the Guide. | It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5 | Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and cryptographic key management processes | 1 | 9 | Clarification | 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. It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity. For example, criticality is referenced in 2.2.2, 2.2.4, 2.3.4.2, 2.4 and 2.5.1 (cloud resiliency, assessment of concentration risk, access management, exit plans and independent monitoring respectively) but not in 2.2.3, 2.3 and 2.3.2 (disaster recovery strategy, ICT security and location of data respectively). This infers that a financial entity would be expected to perform “spot checks” across a wide range of disaster scenarios, encrypt all in transit and at rest data and forcibly locate data for all cloud outsourcing activities irrespective of materiality of the type of service. 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.<br><br>The Guide does not reflect the differing expectations of the ECB regarding different types of cloud services, such as SaaS, PaaS and IaaS. Differing types of cloud services have differing forms of resiliency controls, proprietary technology and roles within a financial entity’s technology stack. In a number of cases, the supervisory expectations of the ECB within chapters are clearly in relation to IaaS technology only. The EU’s Data Act, for instance, outlines clear instances where switching or interoperability between CSPs and on-premises are technically unfeasible and can constitute “significant interference in the data, digital assets or service architecture.” This, notably for cloud services which have a higher level of proprietary technology and therefore less substitutable services, should not be considered a supervisory expectation for all cloud services that a firm outsources. Further recognition of the variety of cloud services that exist should be included within the Guide. | It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 6 | Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data | 1 | 10 | Clarification | 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. It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity. For example, criticality is referenced in 2.2.2, 2.2.4, 2.3.4.2, 2.4 and 2.5.1 (cloud resiliency, assessment of concentration risk, access management, exit plans and independent monitoring respectively) but not in 2.2.3, 2.3 and 2.3.2 (disaster recovery strategy, ICT security and location of data respectively). This infers that a financial entity would be expected to perform “spot checks” across a wide range of disaster scenarios, encrypt all in transit and at rest data and forcibly locate data for all cloud outsourcing activities irrespective of materiality of the type of service. 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.<br><br>The Guide does not reflect the differing expectations of the ECB regarding different types of cloud services, such as SaaS, PaaS and IaaS. Differing types of cloud services have differing forms of resiliency controls, proprietary technology and roles within a financial entity’s technology stack. In a number of cases, the supervisory expectations of the ECB within chapters are clearly in relation to IaaS technology only. The EU’s Data Act, for instance, outlines clear instances where switching or interoperability between CSPs and on-premises are technically unfeasible and can constitute “significant interference in the data, digital assets or service architecture.” This, notably for cloud services which have a higher level of proprietary technology and therefore less substitutable services, should not be considered a supervisory expectation for all cloud services that a firm outsources. Further recognition of the variety of cloud services that exist should be included within the Guide. | It is unclear whether supervisory expectations are for cloud outsourcing (across all SaaS, PaaS and IaaS services) in relation to CIFs or all cloud outsourcing activities of the financial entity. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 7 | Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions | 1 | 5 | Deletion | The Guide 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.<br><br>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. It is unclear what further supervisory guidance is provided by the inclusion of NIS2 and to what extent it could cause interpretation issues due to its lack of applicability to financial services. There is a risk that the inclusion of NIS2 could cause further confusion for the financial sector concerning the lex specialis determination. | **We recommend that all references to NIS2 are removed**. There is a risk that the inclusion of NIS2 could cause further confusion for the financial sector concerning the lex specialis determination. We recommend that all references to NIS2 are removed. | , | Don't publish |
| 8 | Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions | 1 | 6-7 | Deletion | Recommendation to delete the following sentence:<br>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.~~"<br><br>Specific solutions, such as containerization, virtual machine-based applications and encryption methods, should be chosen on a risk-based basis and depending on the needs of the financial entity. Specific solutions often become obsolete with continued innovation and are subject to wider considerations beyond the regulatory intent. A financial sector must consider what is most appropriate for their services, infrastructure and within their risk appetite. We recommend that the Guide is redrafted to not prescriptive specific approaches to technology adoption. | A financial sector must consider what is most appropriate for their services, infrastructure and within their risk appetite. We recommend that the Guide is redrafted to not prescriptive specific approaches to technology adoption. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 9 | 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 | 1 | 7 | Deletion | The Guide 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.<br><br>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. It is unclear what further supervisory guidance is provided by the inclusion of NIS2 and to what extent it could cause interpretation issues due to its lack of applicability to financial services. There is a risk that the inclusion of NIS2 could cause further confusion for the financial sector concerning the lex specialis determination. We recommend that all references to NIS2 are removed. | There is a risk that the inclusion of NIS2 could cause further confusion for the financial sector concerning the lex specialis determination. **We recommend that all references to NIS2 are removed.** | , | Don't publish |
| 10 | 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 | 1 | 9 | Deletion | The Guide 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.<br><br>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. It is unclear what further supervisory guidance is provided by the inclusion of NIS2 and to what extent it could cause interpretation issues due to its lack of applicability to financial services. There is a risk that the inclusion of NIS2 could cause further confusion for the financial sector concerning the lex specialis determination. We recommend that all references to NIS2 are removed. | There is a risk that the inclusion of NIS2 could cause further confusion for the financial sector concerning the lex specialis determination. **We recommend that all references to NIS2 are removed.** | , | Don't publish |
| 11 | Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis | 1 | 4 | Clarification | The risk considerations are unnecessarily prescriptive and expand existing due diligence practices and requirements. Additionally, the Guide does not adequately apply a risk based approach (only references CIFs in reference to consideration of sub-outsourcing risk). DORA and the EBA GLs apply proportionality to their respective requirements surrounding ex ante risk assessments.<br><br>The potential risks associated with a "considerable fall in quality" would be managed through performance expectations in contractual arrangements / in SLAs for critical engagements, and through ongoing monitoring of the service provider's performance. It would be difficult to assess such risks at the onboarding stage. | The ECB guide expands requirements above the scope of DORA and EBA Guidelines. The Guide should expressly state that financial entities should, on a risk-based approach, identify and assess all the relevant risks relating to the outsourcing of cloud services, prior to entering in a new arrangement with a CSP. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 12 | Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions | 1-3 | 6 | Clarification | It is unclear regarding the resilience benefit that would be provided if all ECB-supervised entities had to place their back-ups for cloud hosted applications outside the CSP that originally hosts that service. Depending on the particular cloud service, having a multi-regional cloud back-up within the same CSP would provider a higher level of resilience benefit without any impact to the service should there be a disruption. Enforcing external back-ups, without a risk assessment predicated on plausible disruption scenarios, would result in excessive cost, more operational complexity and limited resilience benefit. The only scenario would be the complete CTC eradication of a CSP, which remains an extreme scenario to account for across all outsourced cloud services.<br><br>**ECB Guide seems to suggest a mandatory multi-cloud strategy**, and this should not be the case - regulatory expectations on multi cloud strategy do not match the real use cases. Multi cloud strategy is not a reasonable approach - it has proven to be too complex and costly:<br>- it does not deliver the expected value in terms of technical efficiency,<br>- it is not cost-efficient,<br>- it is not always feasible in terms of availability of CSPs comparable solutions.<br>- it can introduce increased cybersecurity risk and operational complexity that can reduce the resilience benefit.<br><br>FIA Members express concern on the uncertainty of how to define 'under stress' as mentioned in the ECB Guide (e.g. business continuity management measures should address a worst-case scenario where some or all of the relevant cloud services (provided by one or more CSPs) are not available and the institution has to perform an exit under stress or an exit without cooperation from the CSP(s) in question). We note that the wording on DORA differs as it mentions 'extreme scenarios'.<br><br>FIA Members deem the ECB guidance proposes unrealistic time objectives for exit. It is not realistic and feasible from a technical point of view to exit a CSP in weeks. A best practice would be securing CSP support in exiting its services within months (e.g. 6-12 months) - even in case of switching to another CSP - in alignment with ESMA guidelines. | The ECB Guide would be introducing a new requirement. There is no requirement in DORA to use a backup-up of a different Cloud Service Provider. FIA Members express concern on the uncertainty of how to define 'under stress' as mentioned in the ECB Guide. FIA Members deem the ECB guidance proposes unrealistic time objectives for exit. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 13 | Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions | 1 | 6-7 | Amendment | Amendment recommendation:<br>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."<br><br>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. 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. | 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. 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. | , | Don't publish |
| 14 | Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions | 1 | 6-7 | Amendment | 2.2.2 "The institution should consider the ability to bring data and applications back on-premises depending on the cloud service."<br><br>The Guide 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.<br><br>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. 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. We recommend greater flexibility is applied and that the ECB does not enforce technology infrastructure requirements on financial entities via Supervisory Guidance. | We recommend greater flexibility is applied and that the ECB does not enforce technology infrastructure requirements on financial entities via Supervisory Guidance. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 15 | 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 | 1 | 7 | Clarification | We take note that the ECB understanding is that back-ups of critical or important systems should not be stored in the cloud which hosts the services concerned. The back up procedures and restoration and recovery procedures should be tested periodically in accordance with Article 12(2) of DORA. Tests should be validated as regards the accuracy, completeness, and practicality of recovery procedures.<br><br>In general, FIA Members consider it as a good practice to do backups (e.g. copies for financial entities' critical or important systems data, code, etc.) in different regions or segregated from the hosted services, in order to restore applications and databases in case the main CSP becomes unavailable. This process, however, to establish complete equivalent services with all data and applications being moved takes weeks or longer.<br><br>However, FIA Members believe ECB guidance goes further than the requirements laid out by DORA on this point. FIA Members would like to highlight that testing back up and restoration/recovery procedures is complex and costly. Moreover, the requirement on testing validation is already present in DORA but ECB Guide on testing validation seems to go beyond DORA requirements (e.g. tests should be validated as regards the accuracy, completeness, and practicality of recovery procedures).<br>**Disaster recovery strategy is about leveraging on the resiliency capacity of the given CSP** and not of a 'secondary CSP' (e.g. disaster recovery relies on multi-regions but always within the same provider). Therefore, we agree that disaster recovery should be separated from the production environment, but we disagree on the fact that it should be hosted within another provider. | ECB guidance goes further than the requirements laid out by DORA on back-ups of critical or important systems. This should only be required for storage and should be segregated and not restricted away from the CSP that hosts the services, Examples of restorations in the market have used backups within the CSP, and any enforcement in the Guide would reduce the resilience options available to financial entities. | , | Don't publish |
| 16 | Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks | 1-2 | 8 | Clarification | The concentration risk considerations are overly prescriptive and create additional complexity for FIs. | The Guide should expressly state that financial entities concentration risk should be assessed on a risk-based approach. The Guide could benefit from adopting a flexible and principles-based approach rather than being overly prescriptive. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 17 | 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 | 1-3 | 9 | Amendment | Recommended amendment:<br>2.3: “encryption methods in line with the institution’s data sensitivity classification policy, the type of cloud service and a risk-based approach.”<br>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. | 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. | , | Don't publish |
| 18 | Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data | 1-3 | 10 | Clarification | Data location and processing risks are assessed on a risk-based approach, including in respect of risk-assessment of subcontractors “relevant for” the cloud service. This is vague and does not appropriately apply materiality to the risk management of subcontractors to CSPs. The guidance is too prescriptive and expands existing DORA and EBA requirements.<br><br>Furthermore, the suggestion to “assess additional risks” is not helpful as it broadens the scope of risks to be considered without specifying objective criteria. | The guidance is too prescriptive and expands existing DORA and EBA requirements. Furthermore, the layering of risk considerations adds unnecessary complexity and less focused risk management approach. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 19 | 2.4 Exit strategy and termination rights 2.4.1 Termination rights | 1-2 | 12-13 | Deletion | The Guide significantly expands the scope of termination rights beyond what is currently established in DORA and the EBA GLs. It would be unreasonable to expect the reasons for termination detailed in the guide should be reflected in contractual arrangements with CSPs. This would complicate implementation of effective contracts and does not align with existing risk management and contracting principles and best practice.<br><br>For example:<br>- **the relocation of business units or data centres** 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<br><br>- **changes to national legislation or regulations applicable to data location and processing** 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<br><br>- **significant changes to the management of cyber risk in the subcontracting chain** is covered by general termination rights related to subcontractors under EBA GLs and DORA.<br><br>More specifically, in relation to the below guidance provided in the ECB Guide, FIA Members note this requirement does not reflect risk management practices whereby the notice period for termination has little to do with the transition of services, which is generally for a defined period post the effective date of the termination of services.<br><br>“The institution should ensure that the CSP’s termination rights are aligned with the institution’s exit strategy. In particular, the notice period set out in the contract with the CSP should be sufficient to allow the institution (or any third-party service provider employed by the institution that uses cloud services in its outsourcing chain) to transfer or insource the relevant services in accordance with the schedule in the exit plan.” | As noted above, an outcomes-based approach to supervisory guidance would allow FIs to achieve the same protective outcomes through existing contractual provisions, which are tailored to the specific engagement and operational and risk environments. By focusing on the intended outcomes, FIs can maintain effective risk management while avoiding unnecessary complexity in their contractual arrangements with CSPs. The components of the exit strategy suggested (2.4.2) do not apply a risk-based approach. The expectations on contract termination are overly prescriptive. There could be challenges on how to implement these. | , | Don't publish |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 20 | 2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs | 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.<br><br>Amendment proposed:<br>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…"<br><br>The European Central Bank (ECB) emphasizes that financial institutions should not rely exclusively on monitoring tools offered by Cloud Service Providers (CSPs). Instead, they should complement this information with independent monitoring tools. While we recognise the ECB's intent to ensure there is not a reliance on CSP information, current market availability for independent tools would still require information to be provided by the CSP. In all likelihood, any independent tooling would still be dependent on the CSP. Therefore, the mandatory nature of this requirement should be evaluated with a risk-based perspective. | The ECB Guide would be introducing a new requirement. There is no such specific requirement in DORA. The ECB should not enforce monitoring of CSPs to be undertaken by a single centralised function or a single department within a financial entity. 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. | , | Don't publish |