AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

The European Central Bank's Guide on outsourcing cloud services to cloud service providers

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.7 trillion in 2022, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 56, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive summary

The EU financial sector faces a complex regulatory environment for outsourcing and third-party risk management due to a number of overlapping frameworks, including the incoming Digital Operational Resilience Act (DORA). The European Central Bank (ECB)'s Guide on outsourcing cloud services to cloud service providers (Guide) adds another layer of overlapping requirements and goes beyond the underlying regulations, introducing more detailed and prescriptive expectations. To avoid undermining DORA's harmonisation objectives and creating an increasingly convoluted regulatory environment, the ECB should revise the Guide to provide flexible and risk-based guidance, focusing on proportionate outcomes and ensuring consistency with the DORA level 1 text.

Introduction

The current regulatory landscape for outsourcing and third-party risk management for the EU financial sector is marked by a suite of overlapping guidance under tech-agnostic and tech-specific frameworks. The three European Supervisory Authorities (ESAs) – the European Insurance and Occupational Pensions Authority (EIOPA), the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA) – have all issued guidelines addressing general outsourcing, cloud outsourcing and information and communication technology (ICT) security risk management for certain subsets of the EU financial sector.

This earlier guidance sits alongside the Digital Operational Resilience Act (DORA), which effectively codifies existing EU guidelines under a comprehensive and harmonised framework regulating the sector's use of ICT third-party service providers, including cloud service providers (CSPs). Until the ESAs' guidance is potentially updated in light of DORA, financial entities and ICT third-party service providers captured within their respective scopes must navigate duplicative, overlapping and often, inconsistent rules.

The European Central Bank (ECB)'s Guide on outsourcing cloud services to cloud service providers (Guide) adds yet another layer of overlapping requirements to the multitude of existing guidelines and regulations covering the management and effective governance of outsourcing risk, as well as ICT security and cyber resilience frameworks. However, it also goes further than the underlying regulations it references, combining scoping and requirements from adjacent regulations and guidance, and introducing more prescriptive and granular expectations. A rigid application of all aspects of the Guide would have a material impact on the cloud strategies of financial entities operating in the EU. Prescriptive cloud measures and technology solutions proposed by the Guide could result in less resilient outcomes, restrict firms' ability to innovate and significantly increase both compliance and operational costs. This is notwithstanding the increase in operational complexity and cybersecurity risk that is not discussed within the draft. Such prescriptive solutions include a requirement for entities to maintain parity in on-premises infrastructure with CSPs and to back up all data and applications.

Whilst the ECB's Guide is intended to clarify the ECB's expectations of DORA compliance by ECB-supervised entities, it significantly expands DORA's technical requirements and intended scope. It also does not consistently apply the proportionate and risk-based principles that are embedded within and fundamental to DORA. The 'gold-plating' of requirements for in-scope entities will have a material impact on their cloud strategies across the EU. This adds to the complexity of DORA implementation, particularly for financial entities with multiple branches across Europe that may not fall within ECB.

Finally, the ECB has issued the Guide at a time when both the financial sector and CSPs are working to implement their compliance with DORA's comprehensive requirements before its January 2025 deadline, as they also await the finalisation of crucial technical standards that will inform more detailed compliance obligations. The Guide does not appear to reference or reflect the secondary technical standards developed by the ESAs and published in the *Official Journal of the EU* or to consider the in-development technical standards. In that context, the ECB's Guide adds a further layer of complexity to the already challenging application of DORA's requirements by ECB-supervised entities and a lack of clarity as to how the ECB's supervisory expectations should align with DORA compliance. This will invariably put cloud users and providers at a disadvantage compared to other financial entities and ICT third-party providers that only have to address the DORA requirements. This comes at a crucial time in their compliance journeys amidst what is already a short implementation period.

Recommendations

The ECB should therefore consider revising the Guide to:

- **Provide flexible and risk-based guidance focusing on proportionate outcomes rather than prescriptive expectations.** The ECB should not prescribe specific forms of technology solutions that inadvertently define a financial entity's future technology stack and adoption. We encourage the development of a holistic, risk-based approach to third-party risk management for the EU financial sector instead of the multitude of frameworks currently in place that cover overlapping outsourcing and ICT populations. This would allow financial institutions (FIs) to adapt their risk management frameworks to any cloud-specific or evolving technology risks that the ECB considers as not adequately covered by current regulatory frameworks. In particular, the ECB should:
    - Remove the prescriptive expectation in Article 2.2.1 about not storing back-ups in the cloud that hosts the primary system and instead focus on effective restoration and recovery as an outcome; and
    - Remove the prescriptive expectation in Article 2.2.2. about minimising the impact of using a solution specific to an individual CSP and using virtual machine-based applications and/or containerised applications (which does not technically apply to all system architectures), and instead focus on effective migration as an outcome.
- **Align key definitions to the relevant DORA definitions.**
    - **Critical or important functions:** There is already a significant divergence across different regulations in the terminology and criteria used to identify what is 'critical'. The ECB's Guide currently uses two different definitions of criticality: 'Critical Functions' for which it uses the definition of 'Critical or Important Functions' from the EBA's Outsourcing Guidelines; and 'Critical or Important Functions' for which is uses a slightly amended version of the definition for 'Critical Functions' under the Bank Recovery and Resolution Directive (BRRD). Neither of these is aligned with DORA's definition of 'Critical or Important Functions'. Given the ECB's Guide is purported to reflect the ECB's understanding of DORA and how its requirements apply to the banks it supervises in the context of cloud outsourcing, aligning the Guide's definition to

DORA would provide clarity and consistency to help industry meet supervisory expectations.

- **Subcontractors:** The Guide uses the phrase 'suppliers of subcontracted services supporting the CSP'. This phrase is not used in DORA or the secondary texts. To reduce confusion, the ECB should align the terminology in the Guide about subcontracted services with language in the Implementing technical standards (ITS) on the Register of Information (ie 'subcontractors that effectively underpin the provision of these ICT services').
- **Directive on measures for a high common level of cybersecurity across the Union (NIS2):** It has been confirmed that DORA applies with *lex specialis* status with regards to NIS2 for those areas where they overlap. The ECB's referencing of NIS2 requirements that overlap with the coverage of DORA does not recognise this status, and risks basing the ECB's expectations on an incorrect legislative basis and creating confusion across industry regarding the application of NIS2 and DORA. The Guide should reference the interpretation in regards to DORA and remove all references to NIS2 in order to reduce this uncertainty for the sector.

- **Ensure consistency with the DORA level 1 text and avoid gold-plating.** The Guide is positioned as an explanation of the ECB's understanding of DORA. However, in several cases the Guide either places more limitations on or create additional requirements for financial institutions using cloud services that are not contemplated in DORA. For example:
  - Article 2.2.1 contains an expectation for institutions not to store back-ups of critical or important systems in the cloud that hosts the primary system. This is narrower than Article 12(3) of DORA, which says 'When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system.'
  - Article 2.2.2 contains an expectation for institutions to 'bring data and applications back on premises'. This is narrower than Article 28(8) of DORA, which refers to both 'transfer[ing] them to alternative providers or reincorporat[ing] them in-house'.
  - Article 2.2.3 contains an expectation for institutions to directly tests their CSP's disaster recovery plans (including spot checks and tests on short notice). This goes beyond the requirement to test the financial entity's ICT response and recovery plans in Article 11(6) and creates undue risk for the CSP's other customers, which includes other financial entities.
  - Article 2.4.1 contains additional grounds of termination and termination scenarios that overlap with, conflict with and exceed the grounds of termination in Article 28(7) of DORA.
  - Furthermore, the draft mentions in its scope and effect chapter that non-CSP third-party providers (TPPs) that are reliant on cloud services are expected to fall under the same supervisory regime as the CSP. This expectation is not consistent with DORA; the term 'reliant' gives too much room for interpretation, making this requirement disproportionate for TPPs.

- **Ensure the consistent application of the proportionality and risk-based principles embedded in DORA throughout the Guide.** The Guide applies expectations for the risk management of all types of cloud services without reflecting the varying levels of risk and technical specification relevant to different types of cloud such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). For example: the expectation in Article 2.3.4.1 that institutions agree on individual clauses with the CSP when configuring the cloud environment may be appropriate for SaaS, but it not consistent with the IaaS or PaaS models, where configuration is a customer responsibility and can be changed by the financial institution at will. Additionally, the Guide applies requirements to services supporting critical or important functions (CIFs) in certain chapters but not others. The Guide should include a developed approach to proportionality that is consistent with DORA. Where the Guide intends to capture subcontractors, it should explicitly apply a materiality threshold to supply chain scope in alignment with DORA (ie as noted in the comment above about definitions this should be consistent with what is ultimately reflected in the final draft regulatory technical standard on subcontracting, expected to specifically apply to those subcontractors, which effectively underpin CIFs). This should also apply where the ECB seeks to set expectations for TPPs, which are themselves reliant on CSPs. Without the consistent application of a proportionality and a risk-based approach, the supervisory expectations in the Guide could be interpreted as applying to a very expansive scope of CSPs and their subcontractors.
- **Determine the timing of requirements associated with ECB Guide in a pragmatic way, aligned with overall DORA timelines**. The ECB has not clearly communicated the anticipated timeline for implementation of its expectations. Four supplementary technical standards have yet to be finalised (Register of Information, Subcontracting of CIFs, Threat-led penetration testing and Major ICT incident reporting). To allow the ECB's Guide to reflect both these technical standards and those that have been recently published in the *Official Journal of the EU*, the ECB should defer publication of the Guide until all of the supplementary technical standards are completed. Given the pace of ongoing work on DORA's implementation across industry, the ECB should also allow for an appropriate implementation period.

Conclusion

The financial services industry and its third parties are currently grappling with their implementation of DORA's comprehensive requirements. Industry has highlighted DORA's significant compliance challenges and the tight implementation timeline, and these concerns have been acknowledged by the ESAs. DORA specifically contemplates the types of risks associated with ICT third-party service providers, such as CSPs, and sets out enhanced and harmonised risk management requirements, alongside an oversight framework that is expected to capture those CSPs that pose the most significant threats to the stability of the EU financial sector. Not only does the ECB's approach risks undermining DORA's harmonisation objectives, but additional prescriptive guidance will require EU financial entities to interpret and comply with more expansive, specific and overlapping rules, creating an increasing convoluted and complex regulatory environment.