DORA - Draft RTS

The detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers

September 2023

Executive Summary

AFME welcomes the opportunity to respond to the draft Regulatory Technical Standard (RTS) on *the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers* under DORA (Digital Operational Resilience Act)[1]. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

Our response to this consultation is from the perspective of our bank members, focusing on those issues which are most relevant to wholesale capital markets. We are responding to each of the specific questions set out in the consultation paper, but wanted to raise four overarching points:

1. **The overall approach to addressing regulatory duplication has been back-to-front.**

   While we understand that the ESAs are acting as mandated by the Level 1 text, the RTS on the policy for ICT services supporting critical and important functions introduces overlapping and duplicative regulatory requirements, particularly in relation to the EBA Outsourcing Guidelines. We understand that authorities are aware of the incoming overlap and will be undertaking future mapping exercises to redress such duplications. We are disappointed though that the ESAs did not set out to ensure that the requirements were harmonised from the outset. The approach taken will have serious costs implications for financial entities, and needlessly damage the EU's international attractiveness. AFME looks forward to working closely with the ESAs in future on how to streamline the regulatory burden facing financial entities.

2. **A disparate policy covering only ICT third-party service providers should not be required.**

   The EBA Outsourcing Guidelines include detailed requirements that ensure the policy governing a financial entity's outsourcing and third-party arrangements appropriately defines the principles, governance, responsibilities and processes necessary across the entire third-party service provider lifecycle. This encompasses risks related to the provision of ICT services by third-party service providers. Financial entities' third-party risk management programmes establish an overarching framework that allows oversight to be tailored to the specific risks of a third-party relationship.

[1] https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTS_on_policy_on_the_use_of_ICT_services_regarding_CI_functions.pdf

A disparate policy covering only ICT third-party service providers should therefore not be mandated under the RTS, as this would not provide additional benefit to existing risk management and decision-making processes. Financial entities should be able to rely on and enhance existing policies and standards.

3. **The full suite of DORA requirements should focus on identifying and addressing the relevant risks rather than prescribing specific processes and structures within financial entities.**

The RTS should serve to better inform the principled considerations set out in the existing EBA guidance, which allow a degree of flexibility in how outsourcing requirements are implemented by the financial entity. The RTS instead takes a far more prescriptive approach, including in requiring that certain risk management processes and practices (which are currently part of the entity's risk management framework) are explicitly set out within a firm's ICT policy. We encourage the ESAs to focus any new policy standards on principles and intended outcomes, rather than mandating prescriptive processes, procedures or governance which would not provide additional benefit to existing risk management. AFME reaffirms its view that outcomes-based regulation is the most effective way of ensuring supervisory objectives are successfully met in practice. Again the proposed approach will have serious costs implications for financial entities, and needlessly damage the EU's international attractiveness

4. **A grace period for legacy contracts impacted by the new DORA policy on ICT services is needed for the sake of legal certainty.**

The adoption of the policy for ICT services may require financial entities to review and renegotiate existing contractual arrangements with ICT third-party service providers. Given the very tight timeframes for DORA adoption, we would call on the ESAs to provide for a grace period. Given the potential broad scope of entities considered an ICT service provider, and that the RTS is unlikely to be finalised until Q1 2024 at the earliest, contractual requirements should be applied only on a forward looking basis and financial entities should be permitted to implement any new requirements upon contract renewal, rather than necessitating off-cycle remediation. Without time to implement any new contractual requirements, financial entities could be left with as little as 6 months to overhaul contracts which in many cases could be global group-wide arrangements with providers who are themselves outside the EU. Additionally, contracts linked to intragroup/inter-affiliate services should be subject to a proportionate, outcomes-based application of the RTS requirements.

Please see below our responses on questions 1 – 9. We remain available to discuss further any points raised.

Consultation Questions

Question 1 **Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?**

- The principle of proportionality would be bolstered and embedded in the requirements, if the RTS took an outcomes based approach that allowed financial entities to rely upon and enhance existing third-party risk management policies and procedures with any unique ICT-related considerations. We highlight below a number of specific examples.

- In line with AFME's advocacy during the Level 1 discussions, we support the recognition within Article 1 of the Delegated Regulation that there is a difference in risk profile between a third-party provider and an intra-group provider. As noted within recital 31 of DORA, "*when ICT services are provided from within the same financial group, financial entities might have a higher level of control over intra-group providers, which ought to be taken into account in the overall risk assessment*." The current wording of Article 1 could however be read to mean that intra-group providers are in fact higher risk. The following clarification is therefore recommended: "~~whether the ICT third-party service providers are part of the same group of the financial entity~~ *whether the ICT service provider is a third party, as opposed to being part of the same group of the financial entity*."

- We also object to the inclusion of "*the location of the ICT third-party service provider or its parent company"* within Article 1 as an increased complexity or risk. This fails to take account of the third country provisions established in relation to Critical Third Parties as part of the Level 1 DORA text, under Article 36 on the exercise of powers of the Lead Overseer outside the Union, and in any event the location of the third party is already addressed under Article 4 of the Delegated Regulation. The latter provision is preferred as a more direct replication of the existing EBA Guidelines.

- With regards to Article 2, we seek clarification on whether the term "*subsidiaries*" means subsidiaries only within the EU, as opposed to branches within the EU falling under a subsidiary based outside the EU. Additionally we assume that "*consolidated and sub-consolidated basis*" under Article 2 relates to a financial entity's EU presence.

Question 2 Is article 3 regarding the governance arrangements appropriate and sufficiently clear?

- On the methodology for determining which ICT services support critical or important functions, we stress financial entities are best placed to make a proportionate and risk-based judgment call, given their end-to-end oversight of the service in question.

- Additionally Article 3(5) obligates financial entities to assess whether and how the third party provider has allocated sufficient resources to comply with all legal and regulatory requirements. This fails to recognise the difficulties facing financial entities in going beyond a third-party's assurances. We suggest the wording is amended to: "*the policy referred to in paragraph 1 shall foresee that the financial entity* ~~*assesses*~~ ***has sought assurances*** *that the ICT third party service provider has sufficient resources to ensure that the financial entity complies with all its legal and regulatory requirements."* And in line with AFME's wider points across all four Level 2 consultations, financial entities should be able to demonstrate compliance through use of existing policies across the corporate model.

Question 3 Is article 4 appropriate and sufficiently clear?

- We strongly recommend that the inclusion of subcontractors within Article 4 is removed. Firstly, financial entities may struggle in practice to obtain all the relevant information, and secondly subcontracting is already addressed under Article 30 of DORA, with a separate draft

RTS due later in 2023 to provide further information on the conditions which should be attached to subcontracting of services relating to critical and important services. To avoid confusion and unnecessary overlap, we advise the following amendment in Article 4(1): "*the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall differentiate, ~~including for sub-contractors~~, between:".*

Question 4 Is article 5 appropriate and sufficiently clear?

- AFME has no objections, subject to the assumption that there is no expectation on firms to seek fresh/renewed management body approval for previously approved contractual arrangements. Similarly, we would object to any expectation that approval by the management body would need to be regranted in the event that the service provider makes changes as permitted by the contractual arrangement, for example changing a subcontractor.

- This raises a related broader point, on how financial entities must renegotiate existing contractual arrangements with third party providers to incorporate the contractual provisions set out within Article 30 of DORA. While we recognise the provisions themselves are not within the scope of this consultation, we flag that some tech providers may be reticent to agree all the required contractual terms, leading to extended renegotiation periods, which could be challenging within the implementation period. One potential way to address this would be the adoption of a grace period for the renegotiation of legacy contracts, allowing these provisions to be implemented as contracts mature and come up for renegotiation.

Question 5 Are articles 6 and 7 appropriate and sufficiently clear?.

- The risk assessment under Article 6 aligns with the existing requirements under paragraph 68 of the EBA Outsourcing Guidelines. Confirmation is however sought on whether the existing risk assessment can be relied upon for the purposes of DORA. As noted above, we are strongly of the opinion that there should be no expectation on firms to operationally establish a separate risk assessment, or to put in place a sub-set of metrics specifically aimed at ICT services. Risk assessments should continue to focus at the third-party arrangement level as opposed to on individual deployments of ICT tools or particular vendors.

- Article 7(3) reads as if each and all of the elements listed must be used as part of the process for selecting and assessing the prospective ICT third party provider. It is presumed this was an inadvertent drafting error, as it would be unnecessarily onerous to require financial entities to consider all of these elements.

- We recommend the following amendment to the wording of Article 7(3)(c): "*consider any ~~at least~~, the following elements to be used as part of the process for selecting and assessing the prospective ICT third-party service providers: i. ~~audits~~* ***assessments*** *performed by the financial entity itself or on its behalf*". An audit on a prospective supplier would not reflect market practice and be largely unfeasible.

Question 6 Is article 8 appropriate and sufficiently clear?

- Yes. The requirements in Article 8 align with existing guidance in the EBA Outsourcing Guidelines (paragraph 47) on the approach to and governance of intragroup arrangements, consistent with a harmonised and outcomes-based regulatory approach.

Question 7 Is article 9 appropriate and sufficiently clear?

- AFME views the requirements around TLPT (Threat Led Penetration Testing) to be unworkable. We are aware that many financial entities will not enter into pooled TLPT testing for fear that other financial entities would have sight over sensitive data or information. While we acknowledge the mandate within the Level 1 text, we stress the need for greater engagement with industry and alignment with EBA guidelines where relevant.

Question 8 Is article 10 appropriate and sufficiently clear?

- Article 10(1) currently states that "*The policy [on monitoring of the contractual arrangements] should also specify measures that apply when service levels are not met including, where appropriate penalties*." The use of the word penalty is not seen as appropriate in this context and should be deleted.

- Article 10(1) also requires financial entities to monitor ICT third-party services providers' compliance with requirements regarding the confidentiality, availability, integrity and ***authenticity*** of data and information. It is unclear what is meant by "authenticity" in this context, which is a term that is generally used in the context of biometric data. We recommend this is amended to "***accuracy***" of data and information to align with existing concepts and terminology in EU data protection law and current outsourcing guidelines.

Question 9: Is article 11 appropriate and sufficiently clear?

- The requirement for exit plans on ***each*** ICT service to be periodically tested under Article 11 has caused considerable concern in that this marks a considerable uplift in required resourcing from the current market practice, and may also be impractical depending on the service in question, for example as with Cloud. We propose the following wording as an alternative: "*shall include requirements for a documented exit plan for each ICT service supporting critical or important functions provided by an ICT third-party service provider ~~and their periodic review and testing~~, taking into account possible service interruptions, inappropriate or failed service delivery or the unexpected termination of a relevant contractual arrangement. The exit plan shall ~~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~~* ***be realistic, approved at a high level , tested by the different lines of defence of the organisation, and include analysis of possible risk scenarios***".

- We flag as well that in certain areas of the digital services market, there are in practice few or at times no feasible alternatives. The related exit plan could therefore amount to a firm ceasing the service completely, given it is unlikely they will be able to provide such services in-house. Supervisors should take this into account when reviewing the exit plans developed by financial entities.

- Additionally, we flag that the indicators to be taken into account (*service interruptions, inappropriate or failed service delivery or the unexpected termination of a relevant contractual arrangement*) cannot be measured automatically but only through auditing, adding additional compliance burden.

Contacts

AFME	Andrew Harvey	+44(0)20 3828 2694	andrew.harvey@afme.eu
AFME	Stefano Mazzocchi	+32(0) 2883 5546	stefano.mazzocchi@afme.eu
AFME	Coen Ter Wal	+44(0)020 3828 2727	coen.terwal@afme.eu
AFME	Marcus Corry	+44 (0)20 3828 2679	marcus.corry@afme.eu

About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues. AFME represent the leading global and European banks and other significant capital market players. AFME advocates for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society. AFME aims to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work. For more information, visit https://www.afme.eu/