Association for Financial Markets in Europe

Position Paper

Level 2 deliverables for ESA Joint Committee on DORA

March 2023

Executive Summary

The Association for Financial Markets in Europe (AFME) supports the European Commission's (Commission) proposal ('the proposal') for a '**Regulation on Digital Operational Resilience in the Financial Sector' (DORA).** We believe that the aim of the proposal is a positive effort to harmonise the European financial regulatory framework and enhance the resilience and security of the financial sector. The proposal also provides an opportunity to enhance understanding and transparency between financial entities, regulators, and third-party providers; supporting the objectives of the EU digital finance agenda in promoting innovative and competitive financial services.

As the proposal moves to Level 2 discussions, we have identified a number of recommendations on how to best achieve these overarching aims within the anticipated deliverables for 2023/4. This is intended to provide a high level steer, in advance of AFME responding in due course to the draft Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS). There is also considerable member interest in a number of the guidelines, delegated acts and reports which have been commissioned under the Level 1 text.

Building on our long standing positions, in favour of proportionality, harmonisation and outcomes-focused regulation, we have identified the following recommendations:

- **Directly incorporate and/or ensure consistency with existing Risk Management infrastructure, both regulatory and operational.**
- **Retain flexibility within the requirements to take account of different business models, recognising that firms have varying risk appetite levels.**
- **Remain focused on the systemic impact from incoming DORA requirements, and grasp the opportunities from third country engagement**

In addition, we flag the continuing level of concern within industry over the limited window for implementation, including any necessary contractual renegotiation with designated third party providers. With DORA due to apply from 17 January 2025, there is reduced opportunity for industry to prepare. Having a finalised framework as soon as possible would allow firms to meet the applicability deadline in a more effective way.

1. **Directly incorporate and/or ensure consistency with existing Risk Management infrastructure, both regulatory and operational.**

   Given one of DORA's original aims was to harmonise existing risk management and incident reporting frameworks and protocols, this is unsurprisingly an area where a significant amount of regulatory infrastructure is already in place. Failing to incorporate and leverage what has come before risks creating overlap and duplication without any added-benefit. Where new DORA measures expand the scope of existing regulatory requirements, authorities should seek to be as consistent and harmonised as possible, for example through data fields, terminologies and thresholds.

   AFME flags the following provisions:

   - ***Harmonisation of ICT risk management tools, methods, processes and policies (Art 15):*** There is clear overlap with the EBA ICT & Security Risk Management Guidelines, particularly with regards to the incoming RTS setting out elements to be included in the ICT security policies, procedures, protocols and tools. The EBA guidelines are now well-understood and embedded within industry and are a prime opportunity for authorities to rationalise the incoming DORA burden. Authorities should refrain from seeking to enhance or build upon those existing requirements. Further prescription, especially in terms of access management controls and

detection mechanisms, could curtail or restrict a firm's ability to finesse encryption methods or warning indicators within their own business models and risk appetite frameworks. Additionally, further rules on identity access management should be aligned with the existing Identity Management and Access Controls within the NIST Cybersecurity Framework.

- ***Classification of incidents and cyber threats (Art 18):*** While further clarity on the materiality thresholds for classification are welcomed, there is concern this could lead to a new set of DORA related thresholds, which sit alongside a growing myriad of incident reporting thresholds. This is an area where consistency with wider regulations would be strongly encouraged, including the NIS2 Directive. There is strong support for standardised thresholds as to what amounts to a *major* or *significant* incident across the various regulations. If the authorities are unable to standardise at this stage, in light of DORA's tight implementation timeframes, the RTS should be drafted with a subsequent horizontal review in mind. Any such thresholds must also bear in mind that the same incident can have varying impact on individual firms in light of their risk appetite levels. The thresholds must be subject to other qualifying criteria, which carefully focus on the end outcome, and preventing any systemic threat (this point is expanded further below). Alignment with the NIS2 Directive in terms of reporting timelines would also be encouraged for the RTS under Article 20 on reporting templates.
- ***General Principles (Art 28):*** The EBA's recent work on outsourcing should be directly captured within the DORA measures. We strongly recommend that the DORA Register of Information rely upon the same data fields, data formats and approach to proportionality as the existing EBA Outsourcing Registers. The exercise by the ESAs in October 2022 was noted by members to unveil an additional 16 data fields, which were felt to have little benefit but simply risked confusion with those already in operation, and 11 formatting differences compared to the ECB register template. We strongly encourage the ESAs to adopt the EBA data fields and resulting ECB register template data standards as the foundation of the DORA register. Beyond this, any new net register requirements under DORA should be limited to an "ICT layer" of information, if the ESAs decide that additional ICT-specific information is required. Similarly, the requirements to be outlined under DORA for firms' policies on the use of ICT services, provided by third-parties concerning critical or important functions, should align with both the existing EBA Outsourcing Guidelines and the ICT and Security Risk Management Guidelines. These combined requirements form the basis of a firm's outsourcing and third-party policies and already address ICT services and the necessary governance and diligence checks and controls. A disparate policy under DORA covering only ICT third-party service providers should not be mandated. Furthermore, we recommend that any policy considerations developed under this RTS focus on principles and intended outcomes, rather than prescriptive language or terminology. Additionally, authorities should align these requirements with the approach adopted in other parts of DORA: in particular the recognition that intra-group services should be treated differently from third party services. Removing intra-group services from the scope of the Register of Information would ensure alignment with both the general recognition in the recitals of DORA that the former has a different risk profile, and that intra-group service providers are held out of scope for the designation of critical third parties.
- ***Advanced testing of ICT tools, systems and processes based on threat led penetration testing (TLPT) (Art 26):*** As noted within the DORA text, the TIBER-EU framework provides an important precedent in this field, which is highly regarded by industry. It is recognised that the authorities will need to further set out within the Level 2 RTS which functions under DORA should be subject to TPLT and the conditions for internal testers. There is concern though that building on the testing methodology and approach, especially for each phase of the process, could quickly lead to divergence with the existing TIBER-EU framework. Retaining this as an effective template for DORA related TLPT is strongly recommended. Upcoming RTS requirements should be focused on ensuring applicability of TIBER, as opposed to an enhanced framework.

2. **Retain flexibility within the requirements to take account of different business models, recognising that firms have varying risk appetite levels.**

It is critical that authorities resist the urge to seek watertight requirements that are impenetrable to all forms of risk. Risk management must recognise that disruption will occur regardless of all protections put in place and firms are best placed to assess how to mitigate this disruption. AFME recommends outcomes-focused regulation for this reason, and would caution against requirements which restrict firms in choosing their own risk parameters and how to embed risk management tools within their own business. We also draw a distinction between risk management and business continuity. Prescriptive requirements on the latter may well hamstring firms as they seek to respond to an incident.

AFME flags the following provisions:

- ***Harmonisation of ICT risk management tools, methods, processes and policies (Art 15):*** To ensure where possible an outcomes based approach we caution against additional risk management templates, and especially warn against restrictions on encryption methods and any further stipulations on warning indicators, particularly those relating to anomalous behaviour. Likewise, noting the intention to set out further components for both ICT business continuity plans and ICT response and recovery plans, we call on authorities to enable firms to prioritise their efforts on mitigating the impact from disruption, by recognising that prescriptive requirements may negatively impact a firm's ability to react, or divert resources to less effective, or time-sensitive matters. Remaining outcomes-based, rather than prescriptive, would also help bolster consistency with the Basel Principles for Operational Resilience (POR).
- ***Classification of incidents and cyber threats (Art 18):*** The Level 1 text sets out a list of six criteria for determining the severity of an incident or cyber threat. Three of these (namely criteria *1(b), (d)* and *(e)*) are internally focused and consider the impact in terms of a financial entity's own processes and services. Such factors/information will be available to response teams much earlier than the externally focused criteria, including the geographical spread of an incident or the relative economic impact. In order to ensure prompt notification of potential threats, the internal criteria should have preferred weighting.
- ***Advanced testing of ICT tools, systems and processes based on threat led penetration (Art 26):*** Authorities should not adopt a catch-all approach to TLPT, mandating that all relevant functions require testing within the same exercise or at each exercise, but instead allow firms themselves to identify which of their relevant functions should be focused upon within upcoming testing exercises, to enable a prioritisation based on internal risk assessments.
- ***Key contractual provisions (Art 30):*** The incoming conditions which are to be applied to any permitted subcontracting of critical or important ICT functions or services has caused special concern amongst AFME members. The subcontracting of functions or services may well be part of a risk management strategy, to address potential vulnerabilities or shortcomings. The technical expertise or niche specialism of certain subcontractors may be highly valuable in identifying and implementing preventative action in specific pinch points. Curtailing such business decisions, which should rightly be seen as part of a firm's business model, may compel a contractor or a firm itself to absorb responsibilities to which they are not the best suited, thereby exacerbating rather than mitigating risk. Further restrictions on subcontracting to third country providers would then run against DORA's ambitions to boost resiliency within financial services. Ultimately, the considerations under this RTS should serve to better inform the principled considerations for subcontracting under existing EBA and ESMA outsourcing guidelines, rather than requiring a disparate ICT process.
- ***Harmonisation of reporting content and templates (Article 20):*** The call for flexibility also applies to the upcoming RTS on how financial entities should submit their incident reports to the authorities. An overly prescriptive approach may both divert resources from tackling disruption, and delay notification to the authorities themselves, for example by requiring information in the initial notification which is not typically known in the early stages of an incident. Where possible, the EU should use this opportunity to support the FSB's push for global harmonisation by adopting or aligning with the FSB's proposed templates, in particular the FIRE (Format for Incident Reporting Exchange) template for Cyber related threats.

3. **Remain focused on the systemic impact from incoming DORA requirements, and grasp the opportunities from third country engagement.**

In developing the RTS and other Level 2 outputs, AFME recognises that authorities are to work within the policy parameters of the Level 1 text, as published in the Official Journal (OJEU). There remains though a critical need for the authorities to retain the wider perspective, taking account both of the cumulative impact from incoming DORA requirements and the potential implications from interventions in the supply chains of financial services markets. Unintended consequences are always a possibility within regulatory developments, but there is a particular risk of authorities in the field of operational resilience nudging market participants to coalesce around a narrower selection of tools, providers and contingencies, especially from forced termination of contracts. The result of this herding can be that an incident which does breach the sector's defences will consequently have a much larger ripple effect than would otherwise have been the case.

AFME flags the following provisions:

- ***Advanced testing of ICT tools, systems and processes based on threat led penetration testing (TLPT) (Art 26):*** Given the level of resourcing required within these exercises is intensive, AFME supports the provisions within DORA for supervisory cooperation in such testing. We would encourage the authorities to be ambitious,

going beyond simple sequencing of such exercises, and to secure effective and meaningful mutual recognition of testing results. By this, we call out our concern that authorities may be tempted to slightly tweak preceding exercises in order to justify a fresh round of testing. In determining whether an exercise is equivalent, authorities should consider the underlying risks being tested, rather than for example specific applications. Duplication could also be avoided by focusing such exercises at the parent company level, rather than seeking respective branches to perform repeat exercises.

- ***Harmonisation of conditions enabling the conduct of the Oversight (Art 41):*** It is noted that the authorities will be monitoring how financial entities respond to risks identified in relation to Critical Third Party Providers (CTPPs). Firstly, we flag that this will require financial entities to have sufficient visibility over CTPP testing and any issues identified from live incidents, but we also recommend that remedial action by the financial entity should *only* be sought if the CTPP has demonstrated it is unable to address the issue itself. Otherwise there is a risk of the inadvertent coalescing which is flagged above as financial entities shift to a smaller pool of providers. Further, where a financial entity is to exit a contractual arrangement with a specified TPP/CTPP, it is not reasonable to expect zero disruption, especially given the exit may be occurring within a stressed environment. While simulation testing may help mitigate any disruption there must be a level of reasonableness regarding the extent to which firms can replicate and test all forms of exit.
- ***Centralisation of reporting of major ICT-related incidents (Art 21):*** AFME is in principle supportive of the proposal for an EU hub for incident reporting. We see in this an opportunity for significant rationalisation of the reporting burden, assuming it is underpinned by data sharing agreements between the various authorities, at both EU and national level. This would assist authorities in ensuring they have the same perspective and insights on any incident and alleviate financial entities to focus more on mitigation of any related disruption. AFME looks forward to engaging on the joint report in due course. In advance we would though stress the need to consider the potential systemic impact should the hub itself be subject to an incident or breach, as the reservoir of such sensitive information. Safeguards should explore how the hub would alert financial entities to prevent any wider contagion.
- ***Designation of critical third party providers (Art 31):*** AFME is aware that the ESAs Joint DORA Committee is planning a targeted consultation on CTPPS during May 2023. In advance we flag as an overarching point that failing to focus narrowly on those risks which have the potential to be systemic as part of the designation process will result in a overly large number of CTPPs, whose failure would not necessarily have any systemic impact but where nevertheless the provider may decide to curtail their offering to financial entities in order to avoid the compliance burden. This would see the industry coalesce around a smaller number of providers, or around more limited availability of products/services, thereby exacerbating the concentration risk which is being considered. Further, building on the exemption for intra-group providers, we would welcome specific clarity that financial entities themselves cannot be classified as a CTPP by virtue of providing ICT services to clients or other intragroup entities.

Annex 1: Overlap with Risk Management Guidelines

Topic	Guidelines on Outsourcing	Guidelines on ICT and Security Risk Management	DORA
ICT security policies are discussed within the EBA outsourcing guidelines and should be aligned with existing risk assessment requirements for outsourced ICT providers.	4.31.(j) 12.2.65 12.2.68 13.2.82-84	3.4.1	Article 9(2) Article 15(a)
Access management rights should be aligned with both existing NIST and EBA requirements.	Section 13.3	3.4.2	Article 9(4) Article 15(b)
Business continuity plans and testing should remain in-line with EBA Guidelines and BCBS POR.	Section 9	3.7	Article 11(1) Article 11(6)
Sub-outsourcing guidelines should remain consistent with the EBA.	Section 13.1		Article 30.5
Response and recovery plans should be aligned with existing EBA Guidelines.		3.7.3	Article 11(3)
References to **political risk** should remain consistent with those described by the EBA.	12.2.68.d.ii		Article 15(e)
Any **register of information** should seek harmonisation of data fields, terminology and not be subject to continual change across EBA Guidelines and DORA.	Section 11		Article 28(9)

Annex 2: Deep dive on overlap & inconsistency relating to *Key contractual provisions* for ICT services

No.	EBA GLs (Sect. 13, para. 75)	DORA (Art. 30, para. 2, "*Key contractual provisions*" for ICT Services) (Art. 30, para. 3, "*Key contractual provisions*" for critical or important functions)
1	The outsourcing agreement **for critical or important functions** should set out at least:	The contractual arrangements on the use of ICT services supporting **critical or important functions** shall include, in addition to the elements referred to in paragraph 2, at least the following:
2	a. a clear description of the outsourced function to be provided;	(a) a clear and complete description of all functions and ICT services to be provided by the ICT third–party service provider (…). (Art. 30, para. 2, lit. a).
3	b. the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the institution or payment institution.	
4	c. the governing law of the agreement.	
5	d. the parties' financial obligations.	
6	e. whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in Section 13.1 that the sub-outsourcing is subject to.	(a) (…) indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting. (Art. 30, para. 2, lit. a).
7	f. the location(s) (i.e. regions or countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the institution or payment institution if the service provider proposes to change the location(s);	(b) the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third–party service provider to notify the financial entity in advance if it envisages changing such locations. (Art. 30, para. 2, lit. b).
8	g. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in Section 13.2.	(c) provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data. (Art. 30, para. 2, lit. c).

	Regarding confidentiality: not mentioned in EBA GL 75g, but see also EBA GL Sect. 13.2 para. 84: "Institutions and payment institutions should ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the institution or payment institution (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed)."	(c) requirements for the ICT third–party service provider (…) to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework. (Art. 30, para. 3, lit. c).
9	h. the right of the institution or payment institution to monitor the service provider's performance on an ongoing basis.	(e) the right to monitor, on an ongoing basis, the ICT third–party service provider's performance (…) (Art. 30, para. 3, lit. e).
10	i. the agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met.	(e) service level descriptions, including updates and revisions thereof. (Art. 30, para. 2, lit. e). (a) full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met. (Art. 30, para. 3, lit. a).
11	j. the reporting obligations of the service provider to the institution or payment institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider.	(b) notice periods and reporting obligations of the ICT third–party service provider to the financial entity, including notification of any development that might have a material impact on the ICT third–party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels. (Art. 30, para. 3, lit. b).
12	k. whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested.	
13	l. the requirements to implement and test business contingency plans.	(c) requirements for the ICT third–party service provider to implement and test business contingency plans (…). (Art. 30, para. 3, lit. c).

14	m. provisions that ensure that the data that are owned by the institution or payment institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider.	(d) provisions on ensuring access, recovery and return in an easily accessible format of personal and non–personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third–party service provider, or in the event of the termination of the contractual arrangements. (Art. 30, para. 2, lit. d).
15	n. the obligation of the service provider to cooperate with the competent authorities and resolution authorities of the institution or payment institution, including other persons appointed by them.	(g) the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them. (Art. 30, para. 2, lit. g). (iii) the obligation of the ICT third–party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party. (Art. 30, para. 3, lit. e), iii).
16	o. for institutions, a clear reference to the national resolution authority's powers, especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the 'substantive obligations' of the contract in the sense of Article 68 of that Directive.	
17	p. the unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function, as specified in Section 13.3.	(e) the right to monitor, on an ongoing basis, the ICT third–party service provider's performance, which entails the following: (i) unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third–party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies; (ii) the right to agree on alternative assurance levels if other clients' rights are affected; (iii) the obligation of the ICT third–party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and (iv) the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits. (Art. 30, para. 3, lit. e).

18	q. termination rights, as specified in Section 13.4.	(h) termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities. (Art. 30, para. 2, lit. h).
19		(i) the conditions for the participation of ICT third–party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6). (Art. 30, para. 2, lit. i).
20		(d) the obligation of the ICT third–party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27. (Art. 30, para. 3, lit. d).
21		(f) the obligation of the ICT third–party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex–ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs. (Art. 30, para. 2, lit. f).
22		(f) exit strategies, in particular the establishment of a mandatory adequate transition period: (i) during which the ICT third–party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring; (ii) allowing the financial entity to migrate to another ICT third–party service provider or change to in–house solutions consistent with the complexity of the service provided. (Art. 30, para. 3, lit. f).