AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

First batch of draft regulatory technical standards under DORA

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 European Supervisory Authorities (ESAs) have launched a public consultation on the first batch of policy products under the Digital Operational Resilience Act (DORA), including draft regulatory technical standards (RTS) and draft implementing technical standards (ITS). The American Chamber of Commerce to the EU (AmCham EU) welcomes the opportunity to comment and identifies the following areas for refinement:

- The draft RTS on Information and Communication Technology (ICT) risk management tools, methods, processes and policies:
    - Proportionality and risk-based approach.
    - Flexibility in implementation.
    - Report on the risk management framework.
    - Vulnerability reporting.
    - Risk management framework across numerous functions.
- The draft RTS in relation to the contractual arrangements on the use of ICT services supporting critical functions:
    - Audit of service providers.
    - Access to premises.
    - Due diligence.
    - Contractual clauses.
- The draft RTS on the criteria for the classification of ICT-related incidents, materiality thresholds for major incidents and significant cyber threats.
- The draft Implementing Technical Standards (ITS) on the ICT third party register:
    - Definition of ICT Services.
    - Register of information for ICT services; treatment of the value chain.
    - Use of existing reporting frameworks.

Introduction

The European Supervisory Authorities are building a constructive dialogue with stakeholders on this new piece of legislation. The stakeholders have been asked to provide concrete examples to explain their comments on the individual draft RTS. As a member organisation representing a broad spectrum of both the financial services and the ICT industry, we are not best placed to pull together such examples, as they are sector specific. Instead, our members have provided such examples in their company-specific responses to the consultation. We hope these responses will be of value to the ESAs.

Before providing comments on the individual draft RTSs, we would like to draw your attention to a general observation on the draft RTS that is of particular importance for our members. This relates to

a proposed provision that could have unintended extra-territorial implications and potentially discriminate against ICT providers from outside the EU.

The proposed RTS on the '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' suggests non-EU providers are inherently 'riskier' than EU ones and that financial entities should consider this when conducting a risk assessment. Specifically, the proposal under article 1 of the RTS suggests that the location of an ICT third-party service provider or its parent company is an '[element] of increased complexity or risk'. This is not in keeping with the primary DORA Regulation and the RTS should not suggest that the location of the parent company of the provider per se is necessarily an 'element of higher complexity or risk'.

Section 4(1)(c) of the proposed RTS suggests that ICT third-party service providers located within a Member State need to be differentiated from ones located in third countries. As an alternative, we suggest to draft article 1 in line with the approach taken under existing guidelines issued by the ESAs on outsourcing and cloud, for example, paragraph 31 of the European Insurance and Occupational Pensions Authority (EIOPA) Guidelines on outsourcing to cloud service providers.

Draft RTS on ICT risk management tools, methods, processes and policies

Strong and effective ICT risk management and control frameworks in financial entities are crucial to ensure that EU financial services remain resilient. A financial entity's ICT risk management and control frameworks are unique to each financial entity and reflect their individual structures and organisation. In this respect, requirements which are one-size-fits-all or do not allow for flexibility could invertedly restrict a financial entity's ability to effectively tailor their control frameworks to their organisational structure and risk environment.

Proportionality and risk-based approach

The draft RTS in article 29 should include a risk-based approach to proportionality in accordance with the proportionality principle in the European Banking Authority (EBA)'s Guidelines on ICT and Security Risk Management. This would allow for a greater level of flexibility for financial entities to tailor their approaches to risk management and controls frameworks. A financial entity has differing ICT assets, systems and threats, and it should be able to prioritise how they allocate resources to risk to reflect their individual structure and utilisation of ICT services. All ICT assets and systems in a financial entity have different threat profiles and therefore should not be viewed representing equivalent risk, as this will result in a misallocation of resource by financial entities. Drafting should equally allow for instances where the control required is not technically feasible, such as the scanning of all ICT assets that do not have an IP address or locating a server-less cloud asset to a specific jurisdiction.

Flexibility in implementation

As all financial entities have unique structure and organisation, further flexibility within the implementation is required, particularly regarding the roles and responsibilities across a firm's three Lines of Defence (LoD) where the EBA's clarifications in their draft Guidelines on ICT and Security Risk Management (page 73) provides a clear solution. Article 6(4) states that the responsibility for managing ICT risk should be assigned to a control function, but also that the ICT risk management

function and control function should be segregated and independent. These statements are in conflict. Article 2, in addition, could be interpreted as forcing financial entities to locate their cybersecurity functions within their 2LoD, which would be unfeasible for all forms to implement due to financial entities structuring their LoDs in different ways. Digital operational resilience testing, for instance, is not led by the 2LoD in the majority of financial entities.

Report on the risk management framework

According to the causes listed in article 6(5), the requirements within the RTS for financial entities to report on the risk management framework will likely overwhelm financial entities due to the frequency of reporting being required and the complexity of a financial entity's ICT risk management frameworks. A financial entity's risk management framework is composed of numerous different policies, standards and committees across a number of teams in each LoD. Coordination across all teams, including reviews across governance forums, is a complex and a labour intensive process. The number of causes included in article 6(5), even if they occurred individually only once per year, would outpace the speed in which an entity would be able to produce a full report per article 28. The RTS should be redrafted to require one risk management framework report per year that accounts for the preceding year.

Vulnerability reporting

The ESAs approach to vulnerability reporting in article 10(2)(c) could be problematic for ICT providers as it could require disclosure of zero-day vulnerabilities without actionable information to mitigate risks of a vulnerability. Zero-day vulnerability disclosures risk counterproductively weakening security because it increases the risk of threat actors' learning of the vulnerability and then equipping with them details and targets for exploitation. The ESAs should redraft article 10(2)(c) to reflect commonly-accepted coordinated vulnerability disclosure principles. In particular, ICT service providers – or financial entities where appropriate – should be required to disclose vulnerabilities to customers only if a specific action is required by the customer in response to the vulnerability or if mitigation measures or patches are available.

Risk management framework across numerous functions

The current drafting assumes that a financial entity includes all respective requirements within the RTS risk management framework in one individual team or function. This is rarely, if ever, the case within all financial entities, as different functions often are responsible for different requirements that relate to digital operational resilience. For instance, these could be shared or held within different teams across technology, operational risk, crisis management, or cybersecurity functions, which all interrelate but are not within the same function in a financial entity. The way in which financial entities choose to complete and maintain their ICT operations and documentation may vary between organisations, and we do not believe the exact location should be prescribed. A clarification within Recital 2 could provide this flexibility for financial entities.

Draft RTS in relation to the contractual arrangements on the use of ICT services supporting critical functions

The ESAs have made positive efforts to issue technical standards on the ICT policy that build on existing guidance. In contrast to the principled considerations set out in existing EBA and European Securities

and Markets Authority (ESMA) guidance, the RTS instead takes a far more prescriptive approach. Financial entities (Fes) should be able to leverage existing third-party risk management programs which establish an overarching framework that allows oversight to be tailored to the specific risks of a third-party relationship. The RTS should serve to extend risk-agnostic third-party policy requirements under the existing frameworks consistently with an outcomes-based approach. This would preserve a holistic approach to existing ICT third-party arrangements, in terms of how those risk relationships are assessed, managed and defined in relevant contractual arrangements. Our specific feedback below is focused on potential impacts to ICT-third parties and contract management processes:

Audit of service providers — Requirements surrounding audits should specify a risk-based approach (RTS Article 3.8; Articles 7.1(d) and 7.3(c); Article (9.2)):

It is neither proportionate nor an efficient use of limited audit resources to require a large number of different financial entities to conduct regular independent audits of third-party ICT services – such as cloud services – that implement standardised functionality and controls for financial entities. This would lead to multiple financial entities auditing the same company against similar standards. We recommend that audit requirements specify that the frequency and extent of audits should be commensurate with the level of risk, to reflect proportionate and risk-based principles. The standard should also expressly allow for pooled auditing of services offered to multiple financial entities that are substantially similar. Such pooled auditing will avoid redundancy and enable such oversight at scale to the benefit of institutions and service providers.

Access to premises — Access to ICT service provider premises should be appropriately limited (RTS Article 3.9):

To provide clarity on the scope of appropriate access – especially for multi-tenant cloud services offerings – the proposed standard should expressly acknowledge that such access should be limited to data and premises necessary for services supporting critical or important functions, and it should be without prejudice to the security, confidentiality and integrity of the ICT third-party service provider's performance. It would be inappropriate and disproportionate to require service providers to grant unrestricted access to data and premises for a wide range of bodies (including government bodies) in unspecified circumstances and without a clear link. Indeed, granting such access could unnecessarily increase the security and confidentiality risks to ICT service providers to the financial services sector as ICT service providers will need to provision access to their facilities and data for a range of entities including clients, their representatives and supervisory authorities. Although the draft standard does not expressly provide for such expansive and problematic access, it does not directly state limitations, and a planned acknowledgment of such limitations will increase efficiency of contract administration and access activities.

Due diligence – Due diligence on use of subcontractors should be linked to the contractual arrangement (RTS Article 7(b)):

Paragraph (b) currently appears to require financial entities to enquire about whether an ICT service provider uses of subcontractors generally, rather than their use of subcontractors 'for the proposed contractual arrangement'. It should be made clear that due diligence in respect of subcontractors is required to assess the vendor's use of subcontractors 'for the proposed contract' rather than the vendor's use of subcontractors generally.

Contractual clauses – Article 9(4) of the RTS should not create contracting requirements that exceed the requirements established in DORA:

The procedural requirements under DORA article 30(1) already cover contract documentation, and the RTS should align with these provisions. In particular, it is unnecessarily restrictive to require that amendments to contracts be signed, where the contract already allows for the execution of amendments by other means. If the relevant contractual agreement is accessible and executed by all parties in accordance with the terms of their contractual arrangement, the signature requirement becomes redundant.

Draft RTS on the criteria for the classification of ICT-related incidents, materiality thresholds for major incidents and significant cyber threats

The efforts of the ESAs to maintain emphasis on significant incidents and major threats to not pose significant burden on financial entities and their service providers when they need to focus on handling incidents, are a positive development. However, there are opportunities to further improve the current text to ensure it delivers on this goal.

In relation to the overlaps with requirements under the Directive on measures for a high common level of cybersecurity across the Union (NIS2), given the differences with regards to definitions (ie 'major ICT-related incidents' and 'significant cyber threats' under DORA, and 'significant incidents' under NIS2), we would want to ensure close links to NIS2 incident reporting provisions to reduce the compliance burden for both ICT third-party service providers and financial entities.

It seems that the focus on critical or important functions has been lost in the RTS. DORA Level 1 defines a major ICT-related incident as one that impacts a critical or important function. It is not clear throughout the RTS how this definition is taken into account.

In relation to the materiality thresholds for major incidents and significant cyber threats, the current drafting provides low thresholds for 'significant threats' which would be met by most threats – significant or otherwise. For example, the 100,000 euros threshold would be too low for large entities.

When assessing the impact of an incident which may occur if the cyber threat in question materialises (ie under proposed article 17(1)(c) of the draft RTS), weight should be given to the assessment of incidents relating to the financial entities use of service providers (listed in the second paragraph of article 23(11) of NIS2), pursuant to article 23(3) of NIS2. Clarification on these aspects, within the drafting of proposed article 17(1) of the draft RTS, will be useful to avoid over-reporting by critical ICT third-party service providers (CTPPs) and wide application of this criterion by the financial entities, which would enable both financial entities and CTPPs' focus to remain on cyber threats that are relevant to the NCAs' and ESAs' overall objective of enhancing the resilience of firms and the financial system as a whole.

Assessment of impact on other entities is often not possible and should not be a factor to determine an incident's severity or the materiality of a cyber threat. The current draft requires financial entities to make judgements of how threats may affect 'other financial entities, third party providers, clients or financial counterparts'. Financial entities will not have knowledge of the internal workings, security

measures and mitigations in place for such third parties; they will be focused on their own security measures. This may lead financial entities to conclude that practically any cyber threat may impact at least one other financial entity or client and therefore to categorise it as significant and potentially report it.

Article 9.1(f) and article 17.1(a)(b) expect assessment of impact on organisations outside of the financial entity. This is beyond the capability of a financial entity and could not form part of assessing the criticality of an incident. Furthermore, article 17.1(b) asks FEs to assess the probability of materialisation at other FEs. However, probability depends on a number of factors, including the control framework of the other FE, which is not public information. Financial entities are equally expected to take into account the vulnerabilities of the systems of the other financial entities and third party providers or the persistence of the threat and any accrued knowledge, which are outside of the ability of entities to determine. Any cyber threat analysis should focus on the entity itself and not other third parties or financial entities.

The requirement under proposed article 19 that reports shall 'comprise the same level of detail, 197 without any anonymization' may cause unintended security and market risks. Non-anonymised incident information should not be shared under any circumstances. Therefore, the industry strongly opposes the changes proposed in article 19 and explained in background paragraphs 57-60. Further, sharing with all authorities, including law-enforcement, could expose FEs and providers to considerable security risk.

A system in line with the Level 1 text must be preferred. The industry strongly believes that incidents, including sensitive details, should be anonymised and shared only with relevant authorities, on a 'need-to-know' basis. The FE should be made aware of which authorities or law enforcement agencies receive those details as non-anonymised data on incidents could cause a risk to an entity's security. This would additionally result in highly sensitive information being shared without consideration of the information included. Aggregation and anonymisation can help limit the security and market risk that would follow unintended data compromises that would otherwise cause harm to the impacted financial entity, other financial entities and, where an incident involves an ICT third-party service provider, other users of that provider.

The complexity of the regime will be difficult for FEs to operationalise and will create regulatory conflicts with other jurisdictions. While we understand the logic of the approach taken by the ESAs, other jurisdictions are drafting similar regimes but with different criteria and thresholds. It will not be possible for FEs to classify incidents according to multiple regimes. Therefore, flexibility needs to be included in the ESAs RTS on incident criteria and thresholds that allows FEs to maintain their own internal incident classification system while incorporating the regulatory requirements of the EU and other jurisdictions.

Draft ITS on the ICT third party register

Definition of ICT Services

In contrast to the broad definition of 'ICT Services' introduced in the Level 1 text, the Register ITS introduces a proposed taxonomy of specific ICT services captured in Annex IV. Whilst taxonomies promote a common understanding of terminology and regulatory rules in some circumstances, Annex IV captures services which may not present the type of risk which DORA is aimed at addressing. This

may result in capturing an overly broad scope of ICT services and also introduces a potentially unintended expansion of the scope of ICT services defined in the Level 1 text. We do not believe this is the intention of the ITS as it is our understanding that this expansion falls outside the ESAs intended remit.

DORA explicitly provides for proportionality in the implementation of its requirements. This is particularly important given the broad definition of ICT services in the Level 1 text. To maintain clarity and consistency, we recommend that this taxonomy is removed from the ITS. This will allow FEs to delineate the application of the broad definition of ICT services in the Level 1 text and apply a risk-based and proportionate approach.

Register of information for ICT services; treatment of the value chain

The ESA are making positive efforts to establish register templates with clear objectives, designed to achieve the three primary objectives listed under recital paragraph 3 of the draft ITS. In an increasingly interconnected financial sector, robust ICT risk management is paramount for both ICT third-party service providers (ICT TPSPs) and financial entities. The proposed register provides an opportunity to enhance supply-chain resilience through the effective identification, assessment and mitigation of potential ICT risks and vulnerabilities.

A proportionate, risk-based approach is crucial to achieve the ESAs' intended objectives, allowing financial entities and their ICT TPSPs to focus on managing the most significant risks. Whilst the ESAs adopt a proportionate and risk-based approach for certain aspects of the proposed templates and reporting requirements, there are a number of areas where the application of these principles falls short, leading to an unnecessarily broad supply-chain scope.

As an overarching point, the ESAs note that the ITS applies 'proportionality' to the templates simply based on the number of services provided by ICT TPSPs that the FE relies on. Whilst this is a relevant consideration, we would encourage ESAs to ensure that other risk factors are taken into account and applied consistently across the register requirements. This would include the size and complexity of the legal entity, the criticality of the service and resulting operational risk.

Additionally, a proportionate and risk-based approach has not been sufficiently applied to following aspects of the ITS:

1. The register provides for enhanced reporting requirements for ICT services that support critical or important functions. This reflects the appropriate application of proportionality and risk-based principles as it recognises that such arrangements should be subject to enhanced monitoring and regulatory oversight. However, this approach risks capturing an unnecessarily broad scope of ICT services as it does not take into consideration that not all ICT services supporting critical or important functions carry a level of risk (or importance) to the FE that require enhanced reporting or risk management requirements.

   In order to ensure that the register appropriately captures the varying level of risks that are associated with ICT services supporting a critical or important function, the templates must also reflect information on the materiality of the ICT service supporting the critical or important function. This approach aligns with the risk-based approach set out in the Level 1 text and will reflect a more accurate view of the third-party ICT services which are most relevant for a critical or important function, and for risk management and supervision purposes.

2. The ITS broadly considers any subcontractor linked to an ICT service supporting, or supporting material parts of, a critical or important function as a 'material subcontractor'. However, in order to achieve effective supervision and oversight of ICT risk and dependencies across the supply-chain, this definition must be recalibrated to reflect a proportionate and risk-based approach. It is important to recognise that not every subcontractor linked to a critical or important function presents the same level of risk.

   We therefore recommend that the approach to 'material subcontractor' is limited to capture subcontractors of ICT services supporting a critical or important function providing material parts of the contracted service and whose disruption or failure could lead to a material impact to service provision. This will ensure that FEs and supervisory authorities can allocate risk management resources and focus on monitoring service providers that present the most material risks.

   As a practical point, we also recommend that the requirement that ICT-service providers and all subcontractors provide and maintain a valid Legal Entity Identifier (LEI) is amended to reflect a risk-based approach. Recognising the complexities of vast supply chains, the requirement should be applied only to 'material subcontractors' based on the amended definition proposed above. This approach balances regulatory objectives with the practicalities of navigating extensive supplier networks.

3. The divergence across existing register requirements is significant, and should not be necessary given the commonality of supervisory objectives. The templates introduced by the DORA ITS are even more complex and detailed in structure and information requirements. The ITS states that the register aims to ensure a 'minimum level of content and harmonisation'. However, given the ITS is silent on whether additional fields could be added by NCAs beyond the ultimate harmonised template, there is a risk that the DORA register requirements could be expanded in individual Member States, thereby undermining the fundamental harmonisation objectives of DORA. Given the need to avoid further divergence of EU outsourcing registers, ESAs should explicitly restrict any additions to the template by NCAs and/or require the ESAs to review and approve any additions at EU-level to ensure DORA's objective of harmonised EU framework is maintained and remains manageable.

Use of existing reporting frameworks

DORA creates a complex system of collecting and maintaining information in the form of registries. These requirements come on top of existing legislation that mandates the presence of registries for related purposes, related processes, similar data sets or similarly regulated infrastructure. It is therefore clear that organisations do not begin now with collecting this information but have established processes and infrastructure in place for quite a while. In addition, more legislation is in the pipeline concurrently with DORA that will create additional documentation requirements.

All these documentation requirements need to be seen in unison. They are not only requirements that will apply to financial services. These requirements will apply to financial services, some of them in addition to DORA, but furthermore these requirements will apply also to ICT third party providers either directly or indirectly (contractually via the financial services that the ICT providers service).

To manage the cost and complexity of information collection and to ensure that there is an authoritative 'source of truth' the RTS need to cater for the different structures and provide flexibility on how the registries are implemented. In practice, this means that there should not be a one-size-fits-all approach but rather an 'information objective' of the kind of data that organisations should be

able to compile/make available taking into account their unique structures, business models and different applicable laws.

Unless the RTS provide some flexibility on how the registries are implemented and, for example, allow to refer to other sources of information within an organisation, the requirement to create such registries will result in the same information having to be collected multiple times, in different iterations and through different governance processes that are not driven by a business need to manage risk taking into account each organisation's unique features, but by an exogenous artificial regulatory construct.

Some examples of the multitude of registries and processes include:

- NIS2, GDPR and DORA already each require a registry of security incidents mostly regulating the same infrastructure and the same data sets. The Cyber Resilience Act (CRA) will create additional obligations related to incident reporting and vulnerability management as it relates to digital products.
- DORA mandates a 3rd parties registry, which is to a large degree covered by the sub-processor disclosures obligations under GDPR (Records of Processing Activity-Processor), the NIS2 supply chain requirements and the future SBOM requirements of CRA.
- DORA mandates detailed information on the flow of data across different jurisdictions as part of the operational risk and the security controls related to the ICT processes. Similar requirements are mandated under GDPR for the Records of Processing Activity – Controller and the GDPR Privacy by Design requirements.
- DORA mandates systematic vendor risk assessment and unrestricted audit rights. NIS2 has similar requirements. GDPR mandates audit rights for the infrastructures processing personal data (very similar to those regulated by DORA for the financial services) and systematic vendor risk assessment for processing activities outside the EU (under the Standard Contractual Clauses or any other transfer instrument).

Conclusion

The regulatory and implementing technical standards are crucial to ensure a smooth implementation of DORA and digital operational resilience in the financial sector. The ESAs are making positive efforts to build a constructive dialogue with stakeholders on these new legislations, but certain concerns are yet to be addressed. Amongst others, the ESAs should aim to prevent extra-territorial implications (which are not included in the primary DORA regulation) and consider refinements of the approach to ICT risk management, the prescriptiveness in contractual arrangements, incident reporting, third party registers and the use of existing reporting frameworks.