Brussels, February 2021

BSA Feedback on Proposed Digital Operational Resilience for the Financial Sector (DORA) Regulation

BSA | The Software Alliance (BSA) welcomes the opportunity to provide input to the Commission's proposed Regulation on digital operational resilience for the financial sector ("DORA"). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members[1] are at the forefront of data-driven innovation that is fueling global economic growth by helping enterprises in every sector of the economy operate more efficiently.

BSA's members are leading in cybersecurity and around securing key technological capabilities, including Cloud Computing. Our members provide services across the financial services sector and thus have unique insights into the opportunities and risk management challenges associated with cloud adoption in this sector. BSA and its members support the overall objective of increasing operational resilience of financial services' entities to protect the integrity of the European and global financial system.

However, while BSA supports the development of relevant policy instruments and smart regulation that strengthen cybersecurity in Europe, we strongly encourage the EU to consider how regulation specific to financial services and their cloud providers fit into the broader regulatory ecosystem around cloud adoption and security; including ways that existing regulations may already address key concerns. Cloud service providers can best ensure the operational and security benefits of cloud when there is harmonization of the legal and regulatory obligations that apply to them, including those that apply to systems as complex and important to the global economy as the financial sector.

[1] BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

In this regard, the DORA proposal builds on the guidelines on outsourcing developed by the European Supervisory Authorities (ESA) as well as on existing legislation relevant for the digital resilience of the financial sector, such as the Network and Information Systems (NIS) Security Directive and the General Data Protection Regulation. It will therefore be important that, as the legislative process continues, DORA is aligned with this existing framework without introducing unnecessary duplication, complexity or legal uncertainty and remains future proof in a rapidly evolving technological landscape.

BSA would recommend the following elements to be considered during the legislative process – the first set of comments seek to clarify and streamline overlaps and possible conflicting requirements between DORA and the recently proposed review of the NIS Directive (NIS Directive 2.0); the second set of comments seek to address broader issues identified in DORA.

Overlapping requirements between DORA and the proposed revision to the EU Network and Information Security Directive (2020/0359 - "NIS 2.0")

BSA encourages the co-legislators to take into account the following recommendations:

- **Improve clarity around the hierarchy of financial services and cloud regulations and the NIS Directive 2.0**. For financial services entities, the DORA proposal specifically and clearly defines a hierarchy between its requirements and those in the current NIS Directive but neglects to provide similar regulatory clarity for cloud providers. However, under the NIS Directive 2.0, the distinction between "operators of essential services" and "digital service providers" has been removed, and as a result, financial services entities and cloud providers will be considered providers of essential service and their respective requirements under the NIS Directive 2.0 will significantly converge. The clear delineation foreseen for financial services entities should therefore be extended and reflected with regard to cloud service providers. Cloud providers will be designated providers of essential services under NIS Directive 2.0 as well as ICTTP's under DORA. With Financial entities also designated providers of essential services there is a lack of clarity as to which cloud services will fall under DORA ICTTP supervision and which will be under NISD 2.0 if the thresholds or risk criteria differ.

- **Clarify and harmonize terms and definitions across DORA and NIS 2.0.**
  The definition for critical third-party providers in article 28 of DORA should be clearly defined, and the exact criteria for that designation should be laid out in more detail and not subject to further changes via delegated acts, which would lead to further legal uncertainty.

  Moreover, DORA should refer to definitions and concepts that match legal terminology or are defined in other EU legislation as it would further provide clarity in legal and consistency across EU legislations. For instance, the current DORA proposal refers to "ICT risk" (article 3(4)) and defines it with references to the NIS Directive. While this would be a helpful reference and seeks to ensure better consistency with the NIS Directive, the NIS Directive 2.0 actually removes this reference to "ICT risk" and its definition. DORA also introduces new terms such as "ICT systems," "ICT security tools and strategies," and "ICT related business functions" whose definitions and

scopes are not defined. Defining these terms and ensuring they are consistent with other EU legislations will help refine and clarify the material scope of DORA.

- **Harmonize and avoid duplication for the oversight of cloud providers at the EU level**. The DORA proposal foresees that European financial supervisory authorities alone will designate certain ICT third party service providers as "critical for financial entities" and will therefore be subject to their heightened oversight obligations (Art. 28). At the same time, and as mentioned above, the NIS Directive 2.0 now qualifies cloud services as providers of essential services and are placed under the supervision of the national competent authority of their main establishment in the EU.

  It is therefore important to foresee a coordination mechanism between the Lead Overseer in DORA (which will be one of the 3 European Supervisory Authorities responsible for financial supervision, the "ESAs") and the national competent authorities under the NIS and the NIS 2.0 Directives. In addition, DORA should contain clear provisions to ensure that the Lead Overseer's oversight plans and recommendation do not create overlaps, duplication or inconsistencies with the NIS 2.0 framework - particularly the technical and measures that are to be imposed in accordance with that Directive on entities that also qualify as CTPP. It is indeed key to ensure that the baseline security and resilience level that is to be introduced by the NIS 2.0 Directive is identical to ICT providers throughout the various sectors they operate in. Also, the critical designation and oversight by the Lead Overseer should be limited to the relevant part of the providers' business identified as critical for financial entities, based on a context-specific analysis focused largely on the particular business function that it is helping to support.

- **Adopt a harmonized approach to incident reporting.** As part of broader harmonization efforts, DORA's incident reporting standards (article 17) should use the same language and have the same threshold as those contained in the NIS Directive 2.0.

  Under DORA, financial entities are required to report any "ICT-related incident with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity." This low threshold contrasts with higher notification thresholds under the NIS Directive (and NIS 2.0) and the GDPR and may unfortunately result in legal uncertainty for financial entities, an overflow of notifications, and a decreased efficiency from regulators. Moreover, during the legislative process, alignment of the DORA provisions with these legislations for the purpose of notification timelines will be essential.

Proportionality and coordination will help avoid overlaps, potential inconsistencies, and conflicting requirements between DORA and the NIS Directive 2.0. In addition, BSA encourages the co-legislators to consider the following recommendations:

- **Contractual Arrangements between Financial Entities and Third-Party ICT Service Providers**
  Existing relationships between cloud providers and financial entities are based upon contracts tailored to each unique scenario; DORA's suggested specific contractual requirements (article 27) would limit the contractual freedom of a purely and highly professional B2B sector. Companies should be able to customize their agreements based on their specific needs and risks, and guidance on contractual arrangements should come in the form of guiding principles or industry led initiatives.

  At the same time, in the DORA proposal (article 27), some of the detailed contractual arrangements required between financial entities and their ICT third party service providers go beyond existing standard terms – for instance as they relate to a right to inspect, access and audit or to the need to specify the location where the ICT third party service providers perform their services and process data. These provisions could raise concerns about privacy and security requirements, and other commercial considerations such as business confidentiality.
  Additional clarity on what types of audits would meet the proposed legislation's requirements that regulators have the right to access and inspect cloud service providers, including clarification on whether third party audit reports could meet this requirement would be a helpful addition to the legislation.

  Moreover, the possibility for the Lead Overseer to recommend that ICT third party service providers refrain from subcontracting critical functions to a subcontractor established in a third country, does come with clear criteria as to the standards that these sub-contractors should adhere to. We would welcome further clarification, as well as proportionate requirements as to sub-contracting relationships that are in line with WTO commitments (Art. 31 (1) (d) (iv)).

- **Risk assessments for third party providers**. Requiring detailed risk assessments as suggested in article 25 of DORA prior to engagement with third party cloud providers- particularly based on the firm's location or country of origin- could restrict the number of products available for use, potentially impacting the security and reliability of a financial firm's cloud services. The proposed legislation also addresses the use of third parties by cloud service providers by setting forth specific obligations regarding their engagement and use. These rules could prove difficult to enforce and comply with given the rapidly evolving and global nature of cloud-based services and could hinder cloud service providers' efforts to be as responsive as possible in adjusting their services to meet client needs including in ensuring maximum resiliency and security in a given network.

- **Oversight regime and administrative fees.** The proposed oversight regime in article 38 of DORA should be further clarified, again in pursuit of harmonization with existing and developing regulations and frameworks. Further clarity from the EU around the competencies of the proposed oversight regime, particularly around how charges for administrative fees and penalties for non-compliance will be calculated and assessed would be beneficial. We suggest that fees

charged to cloud providers should not exceed the administrative costs of specific oversight tasks related to DORA.

- **Resilience and penetration testing**. Any requirement for operational resilience and penetration testing by financial entities that include ICT third party service providers need to be assessed against the technological reality of these processes and potential risks. The nature of different cloud environments, which may include multi-tenancy, needs to be duly considered and alternative options also accounted for - to minimize inadvertent risks such as the impact of a simulated disruption on the integrity and security of the operations of other customers.

  Also, while testing is the current practice to assess risk and vulnerabilities, new techniques, for instance enhanced continuous monitoring tools is changing quickly, and improvements to its features could provide real-time awareness of risks and vulnerabilities in the near future, and we are optimistic that advancements in this area will improve resiliency in cloud networks across industries.

* * *

For further information, please contact:

Thomas Boué, Director General, Policy – EMEA

thomasb@bsa.org or +32.2.274.1315