ECIS European Committee for Interoperable Systems

ECIS ivzw-aisbl
Louizalaan 65 avenue Louise Box 2
B-1050 Brussels, Belgium

T/F +32 (0)2 706 24 15
info@ecis.eu
www.ecis.eu

15 February 2021

FEEDBACK ON THE EUROPEAN COMMISSION'S PROPOSAL FOR A DIGITAL OPERATIONAL RESILIENCE ACT

1. BACKGROUND ON ECIS

1. The European Committee for Interoperable Systems ("**ECIS**") is an international, non-profit association of information technology companies founded in 1989 which endeavours to promote a favourable environment for interoperable ICT solutions. For three decades ECIS has actively represented its members on issues relating to interoperability and competition before European, international and national fora, including the EU institutions and WIPO. ECIS' members include both large and small information and communications technology hardware and software providers, including IBM, McAfee, Opera, Oracle, and Red Hat.

2. FEEDBACK ON THE PROPOSAL FOR A DIGITAL OPERATIONAL RESILIENCE ACT

2. ECIS welcomes the European Commission's aim to harmonise and build upon existing EU-level legislation in relation to ICT and security risk management through the Digital Operational Resilience Act ("**DORA**") proposal. Given the current pandemic, it is even more vital than ever that innovation, coupled with digital resilience, are given due consideration by the European Commission. However, the proposal (in its current form) requires clarification and further precision, particularly as it significantly increases the scope of existing financial services regulation and the compliance burden on stakeholders.

Regulatory landscape and potential overlap

3. DORA proposes to broaden the scope of the EBA Outsourcing Guidelines (2019)[1] – from ICT third-party service providers ("**ICTTPP**") performing critical, or important, functions, to focusing on all ICTTPPs (Article 2, DORA). Under the proposal, an ICTTPP means: "*an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, data centres, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication*" (Article 3.15, DORA).

4. Given this broader scope, ECIS believes that it is important that the proposal builds on the existing regulatory framework, without contradiction or duplication for cloud and infrastructure providers. Parties subject to the proposals should be able to comply without any uncertainty or replication of obligations under the existing legal framework. For example, more consideration and clarity is required on DORA's interaction with the Network and information Directive ((EU) 2016/1148), particularly regarding ICT risk management and incident reporting.

Outsourcing – greater clarity on supervision and proportionality of measures including sanctions vis-a-vis the risk posed by outsourcing to the cloud

5. DORA seeks to promote convergence on supervisory approaches to the ICT third-party risk in the financial sector by subjecting ICTTPPs that are critical for financial entities to an EU oversight framework. While ECIS is supportive of a greater need for convergence and clarity on tackling ICT third-party risk in the financial sector, it is unclear how this oversight framework will be structured. As drafted, the proposals outline that the Oversight Forum and Lead Overseer will decide whether a ICTTPP is to be designated as "critical" (Article 28, DORA), but the details on the structure of the Forum or the exact criteria for a critical ICTTPP (other than a list of factors to be taken into account) have not yet been outlined.

6. Similarly, DORA also gives regulators oversight over sub-contracting and sub-outsourcing (Article 31.1(d)(iii) DORA). However, these provisions are not clearly delineated. ECIS believes that further consideration should be given to the sub-outsourcing criteria to ensure that both financial institutions and ICTTPPs have greater clarity on the requirements.

7. In addition, ECIS notes the onerous daily penalty payment for critical ICTTPPs' non-compliance with Article 31.1(a)-(c) DORA, at the rate of 1% of the average daily worldwide turnover in the preceding business year (Article 31.6 DORA). This sanction should be narrow in scope, and subject to a reasonableness provision. It is also vital that any such sanction should be proportionate, and in any event: (i) limited to "up to" a rate of 1% of the average daily worldwide turnover in the preceding business year, and (ii)

[1] *See:* https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

narrowed to concern the ICTTPP's turnover in relation to its in-scope business (under DORA).

Unnecessarily prescriptive contractual provisions

8. Under the proposals, DORA prescribes contractual provisions which must be included in all contractual arrangements relating to the use of ICT services, to enable financial entities to monitor ICT third-party risk throughout every stage of their relationship. However, the introduction of these measures is more prescriptive than the EBA and EIOPA Guidelines on outsourcing and use of cloud service providers, where most requirements for the inclusion of contractual provisions only applied when outsourcing "critical or important" functions. This increases the burden on ICTTPPs and may interfere with parties' ability to negotiate and contract freely with one another (Article 27 DORA).

Technology neutrality towards cloud and importance of interoperability and open standards to avoid lock-in

9. While ECIS welcomes the encouragement of cloud computing in the financial sector, it also recognises that many players may need to adjust their services in order to adhere to the necessary standards. It is vital that technology neutrality towards different cloud models is maintained, not only focusing on public cloud infrastructure of the kind offered by hyperscalers. The hybrid cloud approach, supported by interoperability provisions and open standards, are important for the financial sector to avoid over dependence on one particular vendor.

10. In light of this, it is important to be mindful of (and minimise) any increased costs and greater compliance burdens for smaller players, including cloud computing providers. Although ECIS recognises the need to safeguard the financial sector and adapt cloud provider services to its regulatory framework, it is also aware that more onerous and costly obligations (required for entry or maintenance) may foreclose smaller players. This can, in turn, create competitive concerns and provide a springboard for larger, established providers, who have greater operational and financial resources. As such, the criteria for designating critical ICTTPPs (as outlined in Article 28 DORA), should be objective and proportionate.

Information-sharing arrangements on cyber threat information and intelligence

11. Cyber threat intelligence information-sharing between public and private entities is essential for financial services companies to maintain digital operational resilience. Ensuring the interoperability of threat intelligence feeds is critical for successful threat intelligence as it allows for:

    (i) the sharing and receiving of cyber-threat intelligence within, and also beyond, the financial services company's boundaries;

(ii) the rapid detection of, and preparedness to, respond to imminent attacks by cybersecurity experts.

12. Interoperability enables cybersecurity communities to communicate using a common language which, in turn, enables a better understanding of cyber-attacks. Interoperability and cooperation between public and private entities on threat intelligence feeds has clear benefits for businesses, as they deploy cloud services and cybersecurity solutions and seek to protect against existing and prospective threats.

13. Improving information exchange between financial services companies, information sharing analysis centres and community emergency response teams is key to improving operational resilience. Equally, improving interoperability of threat intelligence information feeds will enable companies to consume greater threat intelligence feeds. These principles can be incorporated into Article 40, DORA. Finally, ECIS would like to note that there are emerging global standards and open source initiatives for the interoperable exchange of cyber threat intelligence information, and these should be taken into account before embarking on any new technical standards.