# ECSDA RESPONSE TO
# THE EUROPEAN COMMISSION CONSULTATION ON
# DIGITAL OPERATIONAL RESILIENCE

## Executive Summary

We strongly support the European Commission (EC) in pursuing the work on operational resilience and extending the resilience expectations to all relevant financial market stakeholders. We believe that this has a potential to increase the overall level of financial stability of the European financial services network and its investor protection.

The ability of a Central Securities Depository (CSD) to build and maintain its operational integrity and the full range of operational capabilities, is a key determining factor to conduct CSD business in due care of financial stability. Hence, CSDs find it important to contribute to the construction of the future European operational resilience framework.

Our views can be summarised around the following main considerations, the importance of which we would like to ask the EC to consider:

1. **Convergence of National Competent Authorities approaches**
2. **Comprehensiveness of the framework and interdependency of actors**
3. **Risk-based approach**

## Detailed considerations

As the questions of the consultation are very entity-specific and target individual financial institutions, as an association, we preferred to pass on our views in a single coherent document, rather than responding to the questions in the questionnaire. Below, we would like to include some more detailed considerations which could be considered by the Commission and other relevant authorities.

## 1. Convergence of National Competent Authorities approaches

CSDs are Financial Market Infrastructures, applying a number of relevant (soft as well as legally binding) requirements in the field of operational resilience. These include:

*At the global level*

- CPMI- IOSCO Guidance on cyber resilience for financial market infrastructures, issued as a complement to the Principles for Financial Market Infrastructures.

*At the European level*

- Cyber Resilience Oversight Expectations for Financial Market Infrastructure (indirectly applied to CSDs through their National Central banks).
- The EU CSD Regulation and its standards (CSDR), including a range of articles covering operational resilience.

CSDR has entered into force in 2014 and explicitly states that its overarching requirement on operational risk applies to 'deficiencies in information systems'. CSDR, unlike other areas of sectoral legislation, contains bespoke cybersecurity requirements. Hence, CSDs are already subject to the specific requirements.

**We welcome the considerations expressed in the European Commission's consultation and the earlier ESA's joint advice[1] that there is a need to focus on achieving a consistent cyber-resilience baseline across the financial sector in proportion to the needs and characteristics of relevant entities.** Most legislation warrants further domestic guidance or supervisory advice, thereby inherently creating a risk of divergence in implementation. In addition, legislation on its own will not be sufficient to ensure a comprehensive and universal, and at the same time precise, response to cyber risks. We **encourage the Commission to focus on those actions which are expected to contribute most to achieving a high-level of supervisory convergence, i.e. harmonise incident reporting and cyber resilience testing frameworks.**

**With regard to cyber resilience testing frameworks**, we believe that the establishment of a common set of guidance for such tests avoiding the creation of a new different TIBER are necessary to ensure coherent application and mutual acceptance of the results. This is particularly relevant for CSDs operating (or preparing to do so) in a multi-jurisdictional environment and subjected to multiple overseers and, thus, confronted with a regulatory fragmented landscape. Such guidance would also create a level-playing field on cyber resilience for regulated entities and infrastructures within the EU. Finally, the scarce cyber resources and experts will be drawn by a high number of administrative tasks related to the divergent and at times multiplicated requirements. This could potentially lead to a delay in response to cyber threats as well as to higher cyber-related compliance costs.

[1] *Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU Financial sector*, JC 2019 26, 10 April 2019.

**ECSDA members believe that coordination of supervisory actions and testing should be a fundamental part of a comprehensive approach**.

## 2. Comprehensiveness of the framework and interdependency of actors

**We would like to stress the systemic interdependence of actors participating in the financial system. In case of CSDs, our cyber security exposure and compliance with requirements is also highly dependent on other and potentially critical service providers.**

ECSDA members strongly support a holistic approach: the resilience of CSDs as critical infrastructure providers is directly dependent on the level of resilience of, for example, national central banks, Eurosystem, SWIFT and other actors. This interdependency of financial service players requires a similar approach for all stakeholders. At all times, the risk of creating a single point of vulnerability and/or failure of the entire system should be avoided, given also the potential for cyber incidents to trigger systemic risks.

In particular, we would like to highlight the direct dependence of CSDs resilience on the level of the Eurosystem's resilience, as on one of the most critical providers of services to CSDs (e.g. for T2 and T2S services). CSDs outsource some critical services to the Eurosystem. CSDR, for valid reasons, ensures that CSDs do not need to apply outsourcing requirements[2] to public institutions. The result is, however, that CSDs have limited possibilities to manage cyber related risks stemming from the service delivery of such institutions.

**In the same vein, there is a need to ensure a comprehensive supervisory framework for ICT service providers.** There is a large degree of concentration amongst such providers, and potential vendor lock-in risk, for financial institutions. In the area of cloud services for example, it would be useful to have further guidance on the oversight framework. It would also help to have definitions on different levels of criticality of service providers' categories that CSDs should consider as critical service providers.

**ECSDA believes that such oversight framework should be tailored to the criticality of such providers, i.e. a distinction should be made between small and systemically important providers.** ECSDA also supports the introduction of an EU certification for ICT third party providers, foreseeing mandatory requirements based on both proportionality and criticality. However, the notion of criticality may need to be clarified further in a consistent way across different guidance and legislation (as it is currently seen from different angles in different requirements).

In the context of roll-out of new technology for example, it would be helpful to have additional guidance or confirmation on the applicability to CSDs of already existing and related guidance for the financial sector (which does not necessarily include CSDs). Finally, we also support the approach of "resilience by design" in any newly developed solution or technology in the post-trade space.

[2] See CSDR art. 30 (5). For more, please also see ECSDA response to the ECB guidance on FMI cyber resilience, 2018.

## 3. Risk-based approach

ECSDA members believe that the policy makers should consider adopting a more risk-based approach in the implementation of operational resilience requirements. We believe that Risk and Cyber resilience experts should have a clear methodology, where a 2-hour Recovery Time Objective (2h RTO) should not be a hard but a soft requirement. The 2h RTO does not consider the specifics of CSDs ultimate responsibilities towards the market and regulators, which is the settlement of transactions of the day, by its end.

**We suggest referencing solid contingency plans when assessing the ability of a CSD to resume and recover operations in the most rapid and safest possible way by the end of the day rather than a mechanical requirement of 2h RTO considering that:**

- **First**, CSDs may not be able to resume operations within 2 hours, because of an external dependency. An external and linked party may be down and (as per the considerations in our previous section) may not be subjected to the same requirements. In that context we also believe that the incident reporting should distinguish between the incidents generated genuinely by the CSD and those generated by external critical providers.

- **Second,** there is a big difference in criticality of different moments during the day, and of different CSD services. Therefore, the CSDs' response – in its focus and assessment of possible recovery actions – should be able to take into account all those elements which would contribute to the most adequate and optimal outcome.

- **Third and more important,** it may be more dangerous (e.g. in the context of a cyber-attack) to resume the operations without thorough investigation.

**Therefore, the CSDs contingency plans should be integrated as a way to assess the capacity of a CSD to resume and recover its operations. Such contingency plans should allow to consider the impact of a cyber incident on the service delivery of a CSD, as well as the tolerance of a CSD for such impact in view of its risk appetite. In our view, this will qualify as a risk-based approach which is preferable over a mechanical approach.**

**We thank you for the opportunity to contribute to the consultation and would be pleased to engage in further dialogue on this response.**

***About ECSDA***

*The European Central Securities Depositories Association (ECSDA) represents 41 Central Securities Depositories (CSDs) across 36 European countries. The list of ECSDA members is available on www.ecsda.eu/members/list-of-members*

*Our EU Transparency Register number is 92773882668-44. For further information, please contact ECSDA Secretariat at info@ecsda.eu or +32 2 230 99 01.*