FESE Digital Finance Simplification Proposals

14th October 2025

Contents

1. Introduction

FESE welcomes the European Commission's Call for Evidence on the Digital Simplification Omnibus initiative. We support the Commission's simplification agenda and its efforts to streamline digital rules in order to reduce administrative costs for businesses, citizens, and public administrations. This response outlines FESE's views on how targeted amendments can enhance legal clarity, alleviate regulatory burdens, and foster a more balanced and agile digital finance framework across the EU. We remain committed to constructive dialogue with policymakers to ensure that digital simplification delivers tangible benefits for market participants while safeguarding investor protection and market integrity.

In particular, regarding cybersecurity, we welcome the Commission's recognition of the significant burden placed on businesses by incident and data reporting obligations, which are regulated under various EU-level rules, both horizontal and sector-specific, and further complicated by national transpositions. In this context, we outline several recommendations specifically aimed at improving the Digital Operational Resilience Act (DORA), as well as its overlaps with other regulatory frameworks. These are further complemented by proposals related to the Framework for Financial Data Access (FIDA). Please refer to the summary below and the attached document for a detailed explanation of our proposals.

DORA:

- **Definition of the ICT services**: exclude standard hardware and software services from standard IT suppliers to reduce unnecessary administration efforts.
- **Financial entities ICT-security awareness programmes:** ensure that it is only the ICT service provider's duty to regularly train their employees in ICT security awareness programs rather than financial institutions.
- **Register of Information**: reassess the areas where the fields of the Register of Information could be simplified and allow consolidation of the reporting obligation for groups of market infrastructures. The register should include a threshold or other objective criteria to determine which contracts must be entered in the register.
- **Major incident reporting:** simplify the reporting obligation for groups of market infrastructures, allowing the possibility to aggregate information for DORA reporting obligations. It is proposed to delete letter d) of Article 7(1), and to delete Article 7(2) of DORA ITS on the reporting of major ICT-related incidents.
- **Subcontracting:** limit the layers of ICT- subcontractors for which requirements must be fulfilled to certain levels of subcontracting (e.g. 3 layers) instead of focusing on the whole value-chain. Primarily concentrate on ICT subcontractors whose failure could have a material impact on the ICT services received by the financial entity.
- **Thread-led penetration testing**: the selection of companies for the TLPT testing should be based solely on their market share in terms of turnover at Union level as stipulated in Article 2(2)(f)(ii)) and not at national level.
- **DORA & NIS 2 misalignment**: enhance alignment between the DORA and NIS2 frameworks, with greater emphasis on developing joint auditing standards, fostering mutual recognition of certifications, and developing standardised contractual terms.
- **DORA & CRA overlaps**: propose a targeted exemption in the CRA for PDEs that are designed and provided by a DORA financial entity to another financial entity as part of the provision of an ICT service within the meaning of DORA.

FIDA:

- **Scope**: reduce the scope of affected entities by excluding CASPs as they are already governed by a comprehensive regulatory framework under MiCA.

2. DORA

2.1. DORA – general

- **Issue:** The definition of ICT services under DORA encompasses highly standardised hardware and software offerings (e.g., firmware updates) delivered by a broad range of globally recognised IT suppliers, such as Hewlett Packard Enterprise, Cisco, and Oracle. The regulatory burden placed on these providers, along with the administrative effort required from financial institutions, appears disproportionate to the intended regulatory benefits. As these services are provided to a wide range of industries, and are extremely standardised, they pose no significant risks. Any remaining risks are more effectively mitigated through rigorous testing procedures and dual-provider strategies implemented by the financial entities rather than the DORA framework.
    - **Proposal:** Adjust the definition of the ICT services to exclude standard hardware and software services from standard IT suppliers to reduce unnecessary administration efforts for regulators, financial entities and standard IT suppliers.
- **Issue**: According to DORA, Art. 30(2)(i), ICT third-party provider shall participate in the financial entities ICT-security awareness programmes and resilience trainings. This is not possible as financial entities are not training enterprises. Furthermore, their tools and applications for staff trainings are usually licenced only for the financial entity and per employee. It is not possible to add hundreds of non-employees with no access to the enterprise network to such training programmes. Furthermore, most of the ICT third-party providers want to get paid per employee for such trainings. It should be in the primary interest of the ICT third-party provider to train its employees on their own in order to provide sufficient quality with their products.
    - **Proposal**: Delete the requirement completely or change it as follows: "it is only the ICT service provider's duty to regularly train their employees in ICT security awareness programs and digital operational resilience training programs."

2.2. DORA – ITS on register of information

- **Issue**: Under DORA ITS on register of information, the requested information is extremely granular and will require significant resources and additional costs to comply. In addition, whilst cross-border groups of financial entities belonging to the same category (e.g. credit institutions) could benefit from simplified reporting requirements (e.g. consolidation of register of information) this is not the case for market infrastructures belonging to the same group since there is no single supervision and consolidation of reporting requirements is not allowed by NCA.
    - **Proposal:** To reassess the areas where the fields of the Register of Information could be simplified. To simplify the reporting obligation for groups of market infrastructures. The Commission could propose the adoption of specific provisions allowing such consolidation that would avoid the duplication of reporting requirements.
- **Issue**: According to DORA ITS register of information, all contracts for ICT services within the meaning of DORA must be recorded. There are many contracts regarding ICT services which involve a relatively low risk and where the contract related amount (service fee) is quite low per annum. It is extremely tedious, and time consuming to obtain and maintain all the relevant information for the register of information for such contracts. The effort this task imposes on financial institutions is overwhelmingly disproportionate to the benefits.

- **Proposal**: In line with the principle of proportionality, the register of information should include a threshold or other objective criteria to determine which contracts must be entered in the register.

2.3. DORA - RTS and ITS on major incident reporting under DORA

- **Issue:** Under DORA ITS on major incident reporting, financial entities located in different member states are not allowed to aggregate incident reports even if they belong to the same group and share the same ICT infrastructures. Amending this framework by allowing trading venues to submit aggregated notifications of incidents would reduce the regulatory burden on entities that operate in several member states and allow for a clearer, more consistent response across all impacted markets. It would also reduce the likelihood of fragmented or inconsistent data being communicated to regulators, which would be provided with a clearer, holistic view of the incident's impact, enabling better detection of systemic risks and faster, more coordinated responses.
    - **Proposal:** To simplify the reporting obligation for groups of market infrastructures, allowing the possibility to aggregate information for DORA reporting obligations. However, it should be considered as a possibility rather than a requirement or obligation. The Commission could propose the adoption of specific measures to enable such consolidation, avoiding duplication of reporting requirements. In particular, it is proposed to delete letter d) of Article 7(1), and to delete Article 7(2) of DORA ITS on the reporting of major ICT-related incidents.
- **Issue:** Article 5(5) of the ITS specifying time limits for the initial notification, and for the intermediate and final reports should also benefit from the principle of proportionality. The reporting deadline during the weekend represents a disproportionate burden, especially in countries with only one stock exchange, where those trading venues are typically small firms with few employees. Therefore, the reporting deadline during the weekend should only apply to companies above a certain size.
    - **Proposal:** As this is an EU-level regulation, the reporting obligation during the weekend for the initial report for trading venues should be classified on the basis of market share in terms of turnover at Union level (see also RTS on thread led-penetration testing (TLPT) Article 2 (2) (f) (ii)) Regulation 2025/1190 and not at national level).

2.4. DORA - RTS on subcontracting

- **Issue:** Regarding the RTS on Subcontracting, this technical standard has already been challenged by the Commission (here) and could include further simplification of the requirements on subcontracting. For example, the Commission deleted Article 5 on Conditions for subcontracting which is a welcome development. However, the provisions concerning the entire ICT subcontracting chain remain extremely onerous and risk undermining the EU's competitiveness. The delivery of ICT services relies on a complex network of third-party providers, each of which may depend on additional third-party ICT services. Unlike outsourcing as defined in frameworks like the EBA Guidelines, DORA subcontracting rules apply to any ICT service supporting critical or important functions — even if not formally outsourced. This broader scope, combined with new sub-outsourcing rules, makes third-party management significantly more challenging and may ultimately prompt ICT providers to withdraw from serving the EU financial sector.
    - **Proposal:** It could be proposed to limit the layers of ICT- subcontractors for which requirements must be fulfilled (e.g. information-, access- and audit rights, due diligence, register of information, etc.) to certain levels of subcontracting (e.g.

3 layers) instead of focusing on the whole value-chain, and primarily concentrate on ICT subcontractors whose failure could have a material impact on the ICT services received by the financial entity.

2.5. DORA - RTS on thread-led penetration testing (TLPT)

Issue: When determining which institutions should be subject to TLPT testing, greater consideration should be given to the principle of proportionality. Especially in jurisdictions with just one exchange, the entities are often small and lightly staffed — making a TLPT requirement disproportionately burdensome. Particularly in companies of a smaller size where all employees know each other, a TLPT (especially with regard to involved employees or if it involves the provision of leg-ups such as access to IT systems) can hardly be kept secret over a long period of time.

- **Proposal:** As this is an EU-level regulation, the selection of companies for the TLPT testing should be based solely on their market share in terms of turnover at Union level as stipulated in Article 2(2)(f)(ii)) and not at national level.

2.6. DORA & NIS2 misalignment

- **Issue**: DORA and NIS2 have introduced cybersecurity frameworks that led to extensive reporting and auditing obligations, with a particular emphasis on third party risk management. However, misalignment between the two frameworks has led to fragmented oversight, and increased compliance burdens. A small number of major ICT providers dominate the market, creating systemic risk and forcing tens of thousands of regulated entities (20.000 DORA regulated entities and 100.000 NIS2 regulated entities) into repetitive negotiations over similar contractual terms. Furthermore, financial institutions and ICT service providers are frequently subject to inconsistent reporting requirements from different national competent authorities (NCAs). Greater alignment between the DORA and NIS2 frameworks would be essential to streamline oversight and reduce duplication.
  - **Proposal**: Creating uniform contractual terms on operational resilience would eliminate the need for thousands of financial institutions to negotiate individually with a handful of key ICT providers. A standardised template on operational resilience criteria would streamline agreements, rendering individual negotiating power of financial institutions irrelevant and ensuring consistent contractual obligations for service providers.
  - To enhance alignment between the DORA and NIS2 frameworks, greater emphasis could be placed on developing joint auditing standards and fostering mutual recognition of certifications.
  - To mitigate systemic risk of provider concentration, oversight should be harmonised via accredited audit regimes based on common standards. While DORA allows pooled audits, accredited audit regimes would allow service providers to mandate an annual audit by an accredited audit firm and to provide the results to its respective regulated service receivers. This would be a significant improvement in comparison to thousands of entities trying to execute the same audits on the same providers.

2.7. DORA & CRA overlaps

- **Issue**: The Cyber Resilience Act (CRA) and DORA both aim to increase the cybersecurity and resilience of the EU economy, one through the lens of products with digital elements

(PDEs) and the other via the ICT systems of financial entities. CRA provides requirements for economic operators of PDEs such as manufacturers and distributors, while DORA focuses on financial entities receiving ICT services. Overlap may arise in specific scenarios, for instance when a product (e.g. software or hardware) constitutes the performance object of an ICT service provided by one financial entity to another, and simultaneously qualifies as a PDE under CRA. In such cases, the scope of both regulations may overlap, potentially resulting in duplicative compliance obligations.

- **Proposal**: Propose a targeted exemption in the CRA for PDEs that are designed and provided by a DORA financial entity to another financial entity as part of the provision of an ICT service within the meaning of DORA.

3. FIDA

3.1. FIDA - scope

- **Issue:** FIDA's expansive scope raises critical concerns about regulatory coherence, extending data-sharing obligations far beyond traditional banking into areas such as insurance, pensions, investments, and even crypto-assets. Especially in the case of crypto-asset service providers (CASPs), it may lead to regulatory fragmentation and overlapping obligations, given that the MiCA Regulation (MiCAR) already provides a comprehensive framework for crypto services. FIDA's data-sharing obligations may conflict with MiCAR's prudential and operational requirements, especially around data protection, custody, and security. Additionally, many crypto services operate on decentralised networks, making the enforcement of standardised data-sharing obligations both technically challenging and legally ambiguous.
    - **Proposal**: Reduce the scope of affected entities by excluding CASPs as they are already governed by a comprehensive regulatory framework under MiCA.