European Economic and Social Committee

ECO/536
Digital operational resilience

OPINION

European Economic and Social Committee

Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014
[COM(2020) 595 final – 2020/0266 (COD)]

Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341
[COM(2020) 596 final – 2020/0268 (COD)]

Rapporteur: **Antonio GARCÍA DEL RIEGO**

Referral	European Parliament, 17/12/2020 Council of the European Union, 22/12/2020
Legal basis	Articles 53(1), 114(1) and 304 of TFEU
Section responsible	Economic and Monetary Union and Economic and Social Cohesion
Adopted in section	12/02/2021
Adopted at plenary	24/02/2021
Plenary session No	558
Outcome of vote (for/against/abstentions)	243/1/4

1. Conclusions and recommendations

1.1 The EESC welcomes the Digital Operational Resilience (DORA) proposal issued by the European Commission, as it aims to bring legal clarity on the ICT risk provisions, reduce regulatory complexity, establish a common set of standards to mitigate ICT risks and facilitate a harmonised supervisory approach, while also providing legal certainty and the necessary safeguards for financial firms and ICT providers. DORA not only enhances the sector's resilience to ICT risks, but is also of interest to a number of stakeholders, including customers, investors and employees, and contributes to the implementation of sustainable development.

1.2 The EESC recommends enhancing the effectiveness of DORA by means of the following steps:

1.2.1 Including within the scope of DORA any provider of critical financial services that develops financial activities and excluding the use of ICT services for non-critical functions.

1.2.2 Ensuring consistency in definition and scope between DORA and the requirements set out in existing guidelines issued by the ESAs.

1.2.3 Regarding ICT Management, favouring a framework focused on a principle and risk-based approach that facilitates the implementation of controls that are future-proof, flexible and proportionate to the risks.

1.2.4 Regarding ICT-related incidents, full alignment with the FSB's Cyber Incident Response and Recovery toolkit.

1.2.5 Regarding digital operational resilience testing, emphasising not only the scale of the financial institution, but also the complexity and critical nature of the service; avoiding mandatory outsourcing conducted by the limited number of external testers, and mutual recognition of testing results.

1.2.6 Consolidating requirements on outsourcing into a single rulebook, in order to enforce legal certainty for all market participants and reliably comply with supervisory expectations.

1.2.7 Fully enforcing lead overseers' recommendations and a clear set of roles and responsibilities for the different authorities involved in the oversight of CTTPs.

1.2.8 Ensuring access to outsourced services that are deemed critical to TPPs established in third countries so as to avoid restricting firms' freedom of contract and the capacity to access the services of high value-added providers.

1.2.9 Including proportionality in the penalty regime to avoid disincentives for ICT providers to serve EU financial entities and moving away from the current reference to worldwide turnover.

1.2.10 Providing clarity on the ability of firms to share cyber-threat information by ensuring that such arrangements are put in place on a voluntary basis and that an explicit provision allowing for the exchange of personal information is included in the DORA proposal.

1.2.11 Raising the exemption threshold of the proposal to micro and small enterprises as defined under Annex I, Article 2.2 of Commission Recommendation 2003/361/EC: enterprises which employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million and reducing the number of requirements applicable to SME entities proportionally to the digital risk profile of the entity could be considered.

1.3 The EESC supports the empowerment of the lead overseers to execute the audit and inspection procedures over the CTPPs, as lead overseers would gain a better understanding of the risks that the CTPPs may pose and this could help to streamline banks' outsourcing procedures.

2. Background

2.1 European consumers and businesses rely increasingly on digital financial services, which goes hand in hand with market participants deploying more and more innovative solutions based on new technologies. The digital transformation is key for the European recovery and for creating a sustainable and resilient European economy.

2.2 In line with the European Commission priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people, the Commission put forward a **digital finance package**. This package outlines measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it.

2.3 In addition to the proposal on digital operational resilience, the digital finance package includes a new strategy on digital finance for the EU financial sector[1] and a proposal for a regulation on markets in crypto assets together with a proposal for a regulation on a pilot regime on distributed ledger technology (DLT) market infrastructure[2].

2.4 **Digital operational resilience** is the capacity of firms to ensure that they can withstand all types of disruptions and threats related to Information Communication Technologies (ICT). The ever-increasing dependency of the financial sector on software and digital processes means that ICT risks are inherent in finance. Financial firms have become targets of cyberattacks, which result in serious financial and reputational damage to consumers and firms. These risks need to be well understood and managed, especially in times of stress.

2.5 While reforms that followed the 2008 financial crisis strengthened the resilience of the EU financial sector, ICT risks were only indirectly addressed. The lack of a comprehensive European-level regulatory framework on digital operational resilience led to a reliance on national regulatory initiatives. This, however, has limited cross-border effectiveness and has led to a fragmentation of the single market, which undermines the stability and integrity of the EU financial sector. Against this background, the Commission proposes to create a comprehensive framework on digital operational resilience for EU financial entities.

---

1 See EESC ongoing opinion ECO/534 – Digital Finance Strategy for the EU

2 See EESC ongoing opinion ECO/535 – Crypto assets and distributed ledger technology

2.6 The **legislative proposal on digital operational resilience (DORA)**[3] aims to enhance and streamline financial entities' conduct of ICT risk management, establish thorough resilience testing of ICT systems, foster information sharing and increase supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities, as well as introduce powers for financial supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers. The proposal also aims to create a consistent incident reporting mechanism that could help reduce administrative burdens for financial entities and strengthen supervisory effectiveness.

2.7 The Commission also presented a proposal for a directive[4] because it is necessary to establish a temporary exemption for multilateral trading facilities and amend or clarify certain provisions in existing EU financial services directives to achieve the objectives of the digital operational resilience proposal.

2.8 Ranking as one of the largest industries in the world, the ICT market was estimated to be worth over five trillion USD in 2019 and over six trillion by 2022. The continuous growth serves as a reminder of the ever-increasing prevalence and importance of technology in today's society. **Finance is the largest ICT user in the world, with about 20% of all total ICT expenditure,** according to the legislative proposal's impact assessment.

2.9 **COVID-19 has driven the proliferation of digital financial services,** as branch networks of financial institutions remain underutilised. This will spur investments in digital self-service tools, open finance applications and value-added services. Overall, the current situation will force financial institutions to invest more in IT infrastructure, prioritise the migration of critical workloads and update existing apps. The European financial sector is already undergoing a major digital transformation and its ability to compete on a global scale will largely depend on the ability of European institutions to benefit from the most advanced technologies.

3. General comments

3.1 **The EESC welcomes the Digital and Operational Resilience (DORA) proposal issued by the European Commission** which addresses many of the claims noted by the financial sector and aims to bring legal clarity on the ICT risk provisions, reduce regulatory complexity and lower the administrative burden resulting from diverse rules that apply to financial entities across the EU. DORA not only enhances the sector's resilience to ICT risks, but it is also of interest to several stakeholders, including customers, investors and employees and contributes to the implementation of sustainable development.

3.2 The EESC sees DORA as an important step towards establishing a common set of standards to mitigate ICT risks and to facilitate a harmonised supervisory approach, but caution should be taken to avoid adding hurdles that could prevent EU financial institutions from being part of the global innovative process.

---

3 COM(2020) 595 final.

4 COM(2020) 596 final.

3.3 The EESC sees it as an overarching goal that EU authorities seek to achieve a proportionate and risk-based regime that provides supervisors with tools to address their concerns, while also providing legal certainty and the necessary safeguards for financial firms and ICT providers.

4. Specific comments

4.1 Scope and regulatory overlapping issues

4.1.1 Inclusion of additional relevant financial market participants

While the EESC acknowledges and welcomes the broad scope of financial market participants targeted by the proposed legislation that will ensure the consistent application of its requirements across the EU financial sector, we recommend that EU policymakers include financial participants that are not considered part of the scope of this proposed legislation – such as mortgage credit providers and consumer credit providers – to an appropriate degree determined by the risk they may pose to the system. Every provider of financial services that is developing the same activities and taking the same risks should be covered by the same rules and supervision to ensure the same minimum framework for digital resilience that protects consumers and financial stability.

4.1.2 Consistency at international and EU level, as well as with existing regulations

It is crucial to provide clarity to firms, particularly to those operating across borders, ensuring that definitions and terms are consistent and avoiding duplications, overlaps and different interpretations of how to meet similar regulatory expectations in different jurisdictions. The EESC recommends that EU policymakers amend the definition of operational resilience to be consistent with the Basel Committee on Banking Supervision (BCBS) definition[5] and to ensure that it is the leading regime applicable to EU financial institutions to avoid the risk of contradictions with others. Besides, many of the principles and requirements set in DORA are already defined in the existing guidelines on outsourcing[6]. ICT risks and security risk management requirements are also already defined in the EBA Guidelines. It will be crucial to ensure consistency in definition and scope between DORA and the requirements set out in the existing guidelines in order to achieve the harmonisation of EU regulatory requirements.

4.1.3 Equally, the EESC recommends that the EC make sure that the ongoing review of the Security of Network and Information Systems (NIS) Directive and the proposal on DORA share the same definitions and requirements on security incident reporting policy for financial entities.

4.2 ICT risk management

Some elements of the framework are overly focused on compliance rather than on how firms can demonstrate outcomes in a principle- and risk-based approach. Since they are too prescriptive and detailed, they run the risk of becoming obsolete over time as the cyber and ICT

5 Basel Committee on Banking Supervision, *Principles for operational resilience*, 6 November 2020.

6 Such as those produced by the EBA, EIOPA as well as the draft ESMA guidelines which were under consultation.

risk landscape evolves. The EESC recommends a more principle- and risk-based approach that facilitates the implementation of controls that are future-proof, flexible, proportionate, and commensurate to the risks.

4.3 ICT-related incidents

The EESC recommends full alignment between the recently published Cyber Incident Response and Recovery (CIRR) toolkit[7] by the Financial Stability Board (FSB), which provides best practices for incident reporting and the proposed management, classification and reporting of ICT-related incidents envisaged in DORA. There are overlaps that create regulatory uncertainty and increase the regulatory burden for firms.

4.4 Digital operational resilience testing

4.4.1 Although the EESC welcomes the pan-European Threat Led Penetration Testing (TLPT) regime across the EU, as it will increase efficiency and reduce fragmentation, the EESC recommends that authorities focus not only on the size or the scale of the financial institution, but also on the complexity and criticality of the service, taking into account the proportionality principle, where appropriate, to eliminate the distinction between basic testing for all financial institutions and more advanced testing for significant financial institutions, and making sure that customers from smaller financial entities are equally protected and that a level playing field is created among all financial entities.

4.4.2 The EESC recommends that outsourcing testing to external testers should not be made mandatory, as external testers are limited in number. Indeed, firms may have their own in-house testing teams that are familiar with the firms' environment and are able to quickly pivot to more advanced and targeted tests.

4.4.3 The inclusion of ICT third-party service providers within the remit of TLPT should be reviewed. The fact that ICT third-party providers may serve a number of clients could result in significant duplication of testing, which could in turn create relevant risks for the ICT third-party provider and the clients they serve.

4.4.4 Moreover, the EESC recommends making explicit reference to the **mutual recognition of testing results,** given its role in reducing risk and ensuring the smooth functioning of the single market, as well as to avoid cost increases for financial entities operating across borders.

4.5 Management of ICT third-party risk and oversight framework for critical third-party providers (CTPPs)

4.5.1 Ensuring consistency with the existing guidelines on outsourcing

The EESC welcomes the fact that DORA establishes a common regulatory framework for the sound management of ICT third-party risks for all financial market participants across Europe.

7 Financial Stability Board, *Final Report on Effective Practices for Cyber Incident Response and Recovery*, 19 October 2020.

However, it will be crucial to ensure full alignment between this common ground set out in the key principles (articles 25, 26 and 27) and existing rules such as the European supervisory authorities' (ESAs) Guidelines on Outsourcing (i.e., solving the existing dichotomy in scope between "outsourcing" and "third-party service"[8]). Furthermore, we believe this is a great opportunity for EU authorities to consolidate the requirements on outsourcing into a single regulation – with a sufficient level of detail to avoid differences of interpretation – that could bring legal certainty to all market participants and to reliably comply with supervisory expectations.

4.5.2 Requirements applicable to critical or important outsourced activities

In the application of its own Art. 25.2, in order to keep a risk-oriented focus, the regulation needs to be more specific on how the principle of proportionality will be applied, specifying the requirements that would be applicable to critical or important outsourced activities and those that would be applicable to the rest[9]. The EESC recommends that the use of ICT services for non-critical functions should fall outside the scope of DORA.

4.5.3 Direct oversight framework for critical third-party providers (CTPPs)

The EESC welcomes the introduction of a direct oversight framework that will allow for continuous monitoring of the activities of CTPPs by financial authorities, in the absence of an EU horizontal sector-agnostic framework. In the proposed regulation, EU authorities should recognise that when a critical ICT provider comes under this supervision, the risk exposure of financial institutions decreases due to continuous monitoring of their activities. Therefore, this new oversight framework should also help to streamline banks' outsourcing procedures by alleviating some of the burden currently faced by financial entities, for example in relation to the performance of audit and inspection procedures concerning the TPPs that are deemed critical.

4.5.4 The EESC supports empowering the lead overseers to execute the audit and inspection procedures over the CTPPs, as lead overseers would gain a better understanding of the risks that the CTPPs may pose by having first-hand knowledge of their processes and premises, instead of relying on the current reporting provided by the supervised financial institutions and inspections undertaken by national competent authorities. Although the risk mitigation policies of financial entities should be maintained, and the legal obligation remains with them, if inspection and audits are already executed by the lead overseer, financial institutions should benefit from this additional level of security and not have to perform them again.

---

8 DORA refers only to "ICT TPP services" with regards to the key principles for sound management of ICT third-party risk (Chapter V), while the scope of the EBA Guidelines on outsourcing arrangements is based on the definition of outsourcing which implies that the activity is performed on a recurrent or an ongoing basis (par.26). EBA Guidelines also set a list of exceptions that are not considered outsourcing (par. 28).

9 Again, it will also be crucial to align the definition of "critical or important functions" in both DORA and the EBA Guidelines on Outsourcing. In particular, the EBA Guidelines define the factors that financial institutions should consider when assessing whether an outsourcing arrangement relates to a function that is critical or important (articles 29, 30, and 31).

4.5.5 **Lead overseer and national competent authorities**

Once the oversight process has been completed, the lead overseer's recommendations will be followed up by the national competent authorities, which may have their own approach on how to implement the findings of the lead overseer for designated CTPPs. The EESC recommends providing full clarity on the roles and responsibilities of the different authorities in order to avoid a situation where disparity of interpretations affects each of the CTPPs' customers differently depending on their competent authority and thus reduce the risk of fragmentation. These recommendations should also be made fully enforceable, bearing in mind the current ambiguity of Art. 37 as to their binding nature.

4.5.6 **Suspension of a CTPP**

DORA gives national financial regulators the power to require customers to temporarily suspend or discontinue the use of an ICT provider until the risks identified in the recommendations have been addressed. Requirements for any immediate termination of work with a CTPP would definitely impact existing or future business and commercial decision-making (e.g. deterring investments in the EU) and potentially impact financial stability. Before taking this decision, competent authorities should carefully consider, among other factors, the potential negative impact of terminating the service for the financial entities using this particular CTPP[10], set clear criteria for such a requirement and contemplate potential remedies.

4.5.7 In addition, we recommend that if this is ultimately the situation, financial entities should be informed well in advance and should be given sufficient time to exit.

4.6 **Preserving European financial firms' global competitiveness**

4.6.1 The new framework needs to preserve European financial firms' ability to access at least the same technologies as their global competitors. EU financial firms are competing on a global scale and the EU's upcoming regulatory framework should not be putting those EU businesses at a disadvantage by limiting their access to the most advanced technologies – as long as the providers of these technologies meet the EU standards when it comes to resilience and security.

4.6.2 **TPPs established in third countries**

The regulation should not limit the possibility of outsourcing services that are deemed critical to TPPs established in third countries. This limitation would definitely restrict individual entities' freedom of contract and the capacity of European financial institutions to access the services of high value-added providers that most likely will not be found in Europe in sufficient number. This is even more relevant as the proposed oversight framework is limited to the financial

10 One of the criteria to designate an ICT provider as critical would be the degree of substitutability of the TPP, taking into account the lack of real alternatives or the difficulties of partially or fully migrating the services (article 28.2). If this was the case, it would be difficult for financial institutions to port the service to another provider. In addition, requiring exposed financial institutions to move to another service provider would in the end contribute to increased concentration in the European market which would specifically go against the intention of this regulation.

sector, creating an uneven playing field for other players not subject to this regulation, and could end up increasing the risk of concentration, which DORA seeks to avoid.

4.6.3 Punitive penalties based on global turnover

DORA includes punitive penalties with reference to worldwide turnover for ICT providers if they fail to comply with requests by EU financial supervisors. A disproportionate application of those penalties could deter global ICT providers from serving EU financial firms, which could, de facto, limit the choice of providers EU financial firms could have. Additionally, it would deter non-critical third-party providers (non-CTPPs) from opting in to the oversight regime given the fear of being penalised with disproportionate fines and therefore reducing competition in the upstream market. The EESC advocates for the introduction of a level of proportionality in the penalties regime, which is key to avoid disincentives for ICT providers looking to provide services to EU financial entities.

4.7 On information sharing arrangement

4.7.1 As a timely exchange of information is vital to efficiently identify attack vectors and isolate and prevent potential threats, the EESC welcomes the provision for facilitating the establishment of cyber threat information sharing arrangements among financial institutions on a voluntary basis.

4.7.2 We also recommend that EU authorities provide an explicit basis to allow the exchange of personal information (such as IP addresses) among the conditions of this proposal, as this would reduce uncertainty and boost financial entities' capacity to enhance their defensive capabilities, better identify threats and reduce the risk of contagion between them. Further clarity is needed due to the confidential/sensitive nature of the data.

Brussels, 24 February 2021

Christa Schweng
The president of the European Economic and Social Committee