EU Regulation

DIGITAL OPERATIONAL RESILIENCE FOR FINANCIAL ENTITIES

cep**PolicyBrief** No. 2021-11

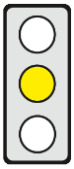
Centrum für Europäische Politik
FREIBURG | BERLIN

KEY ISSUES

Background: The dependency of financial entities on information and communication technology products and services, including from third parties, has increased and creates new risks for the whole financial system. The Regulation addresses those new risks.

Objective of the Regulation: The Commission wants to raise the digital operational resilience of financial entities.

Affected parties: Financial entities, ICT third-party service providers.



Pro: (1) EU requirements to foster the digital operational resilience of financial entities are justified because the products and services delivered by financial entities are critical for the functioning of a society.

(2) Reporting cyber incidents has substantial external benefits. The obligation on financial entities to report them is therefore appropriate.

(3) Establishing an EU oversight framework for critical third-party service providers of ICT may help foster the operational resilience of the financial sector.

Contra: (1) The Regulation lacks proportionality and focus.

(2) Dividing supervisory tasks between EBA, ESMA and EIOPA, may confront critical ICT TPSPs with different and conflicting supervisory approaches. This could be prevented by establishing a joint body of the three Authorities.

The most important passages in the text are indicated by a line in the margin.

CONTENT

Title

Proposal COM(2020) 595 of 24 September 2020 for a **Regulation on digital operational resilience for the financial sector**

Brief Summary

- **Context and objectives**
  - According to the European Systemic Risk Board (ESRB), the high level of interconnectedness of financial entities and the interdependencies of their information and communication technology (ICT) systems may “constitute a systemic vulnerability”. In fact, cyber incidents could quickly spread from a single financial entity to the entire financial system. [Recital 3]
  - However, current EU financial sector law mainly focuses on the main categories of financial risk such as credit, market or liquidity risk, and does not adequately tackle ICT risks [Recital 12].
  - Consequently, the Regulation consolidates and upgrades existing EU ICT risk requirements aimed at financial entities in order to establish a "high common level of digital operational resilience" [Art. 1, Recital 12].
  - To achieve this, the Regulation mainly lays down [Recital 12, Art. 1]
    - requirements for financial entities regarding, in particular,
      - the management of ICT risks [Art. 4–14] and
      - the reporting of significant ICT-related incidents to the competent financial authorities [Art. 15–21],
    - requirements on contracts between financial entities and third-party service providers of ICT (ICT TPSPs) [Art. 25–27],
    - a supervisory framework for critical ICT TPSPs that serve financial entities [Art. 28–39].
- **Scope**
  - The Regulation applies to [Art. 2, Art. 3 (1) (15)]
    - banks, trading venues, investment funds, insurances, and certain other financial entities as listed in Art. 2,
    - ICT TPSPs, i.e., undertakings that provide "digital and data services" such as cloud computing and data analytics services.
  - Financial entities having less than 10 employees and € 2 million turnover and/or balance sheet total (“microenterprises") are exempted from some of the ICT risk management rules [Recital 34, Art. 4–13].

Authors: Dr. Martina Anzini and Philipp Eckhardt eckhardt@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Germany | Telephone + 49 761 38693-0 | www.cep.eu

- **Management of ICT risks**
  - Financial entities must have in place governance and control arrangements that are fit to address ICT risks in an "effective and prudent" manner [Art. 4 (1)].
  - Financial entities must have in place a "sound, comprehensive and well-documented" ICT risk management framework [Art. 5 (1)]. Their management bodies must define, approve, oversee and be held accountable for compliance with the framework. This includes [Art. 4 (2)]
    - identifying clear responsibilities for ICT-related functions within the entity, and
    - fixing the level of ICT risk that the entity accepts as appropriate, in line with its overall risk appetite.
  - The ICT risk management framework must protect all relevant physical components and infrastructures – e.g. hardware – and all relevant premises and data centers from risks [Art. 5 (2)].
  - It must be reviewed once a year, upon the occurrence of major ICT-related incidents and following supervisory instructions [Art. 5 (6)]. It encompasses an ICT multi-vendor strategy that shows and justifies dependencies on ICT TPSPs [Art 5 (9) (g)].
  - ICT risk management must include inter alia:
    - the use and maintenance of updated ICT systems, protocols and tools [Art. 6 (1)];
    - the identification of ICT-related business functions, sources of ICT risks and dependencies on and interconnections with ICT TPSPs [Art. 7],
    - the protection from and prevention of ICT risks, including the adoption of strategies and tools which ensure the "resilience, continuity and availability of ICT systems" and "high standards of security, confidentiality and integrity of data" [Art. 8],
    - the adoption of an "ICT Business Continuity Policy" to allow for quick and appropriate responses to all ICT-related incidents to minimise their impact and trigger immediate resumption of activities [Art. 10],
    - the adoption of a backup policy, specifying which data should be subject to backups and how often such backups should occur [Art. 11], and
    - the adoption of communication plans to inform clients and counterparts and, where appropriate, the public in a responsible manner about ICT-related incidents and vulnerabilities [Art. 13].

- **ICT-related incidents reporting**
  - Financial entities must have a management process in place to detect, handle and disclose ICT-related incidents [Art. 15 (1)]. Such process must include the tracking and classification of the incidents and the division of tasks and responsibilities for taking actions in those situations [Art. 15 (3)].
  - Financial entities must report "major" ICT-related incidents to
    - their competent financial authority, through the filing of an incident report, which must disclose all relevant information to determine the significance and possible cross-border impact of the incident [Art. 17 (1)], and
    - their service users and clients, if incidents have or may have an impact on their financial interests [Art. 17 (2)].
  - The European Supervisory Authorities (ESAs) must adopt draft regulatory technical standards (RTS) that set up the thresholds for determining when incidents are "major", and templates for the reports [Recital 22; Art. 16 (2) and Art. 18].

- **ICT third-party risk**

  Contracts of financial entities with ICT TPSPs
  - Financial entities that use ICT services of TPSPs remain responsible for complying with the Regulation [Art. 25(1)].
  - As part of their ICT risk management, financial entities must manage ICT third-party risk in line with the proportionality principle, taking into consideration the relevance of ICT-related dependencies and the risk arising from contracts with ICT TPSPs for the financial entity's activities and services [Art. 25 (2)].
  - In line with the above, financial entities must, inter alia,
    - before concluding a contract with an ICT TPSP, assess whether it covers a critical or important function, and whether the contract may increase ICT concentration risks, e.g., by checking whether substitutability is maintained or whether multiple contracts with the same provider have been concluded [Art. 25 (5), Art. 26],
    - ensure that contracts on the use of ICT services are terminated, e.g., in case of breaches by the ICT TPSP of applicable laws, regulations or contractual terms [Art. 25 (8)],
    - put in place an exit strategy allowing them to cope with failures or inappropriate provision of services by the ICT TPSP; such strategy must ensure that a contract termination does not impair compliance with regulatory requirements or the continuity and quality of the service offered by the financial entities [Art. 25 (9)].
  - Contracts between financial entities and ICT TPSPs must clearly lay down the rights and obligations of each party [Art. 27 (1)]. They must include [Art. 27 (2)]
    - a description of the services to be delivered by the ICT TPSP, including whether sub-contracting is allowed,
    - references to the location where services are provided and data is processed and stored,
    - qualitative and quantitative targets regarding service levels, and
    - the right of the financial entity to monitor the ICT TPSP's performance, including via on-site inspections.

– Financial entities and ICT TPSPs shall consider making use of standard contractual clauses developed by the Commission to make compliance with the above regulatory requirements more likely [Art. 27 (3); Recital 55].

EU supervision of critical ICT TPSPs

– The Regulation establishes an EU oversight framework for "critical" ICT TPSPs. [Art. 28 (1)].
– Their criticality depends on several criteria, including [Art. 28 (2)]
  - the systemic impact of possible large-scale operational failure by the relevant ICT TPSP on the stability, continuity and quality of the provision of financial services,
  - the systemic importance of the financial entities using the services of the relevant ICT TPSP, and
  - the extent to which the relevant ICT TPSP can be substituted.

  The Commission may add further criteria through delegated acts [Art. 28 (3)].
– Critical ICT TPSPs are designated as such by a Joint Committee of the ESAs [Art. 28 (1)].
– The Joint Committee also appoints, for each critical provider, either the European Banking Authority (EBA), or the European Securities and Markets Authority (ESMA), or the European Insurance and Occupational Pensions Authority (EIOPA) as Lead Overseer. The specific ESA to be appointed by the Joint Committee is the one supervising the most represented financial entities in the client portfolio of a critical ICT TPSP. [Art. 28 (1)].
– The Lead Overseer must assess whether critical ICT TPSPs appropriately manage the ICT risks that they pose to financial entities, e.g., with respect to data security or the physical security of datacenters. It adopts every year for each provider a detailed oversight plan. Once such a plan has been adopted, competent financial authorities are only allowed to adopt measures vis à vis ICT TPSPs if agreed upon with the Lead Overseer. [Art. 30]
– The Lead Overseer may address recommendations to critical ICT TPSPs regarding the use of specific ICT security requirements or on refraining from concluding certain subcontracts [Art. 31 (1)]. The providers must inform the Lead Overseer within 30 days whether they intend to follow a recommendation [Art. 37 (1)].
– Competent financial authorities may force financial entities to suspend their contracts with the providers until the latter address the risks identified in the recommendations. Where necessary, the authorities may also require financial entities to terminate their contracts. [Art. 37 (3)]
– Financial entities must not make use of ICT TPSPs established outside the EU if such providers would be classified as critical were they to be established in the EU [Art. 28 (9)].

Statement on Subsidiarity by the Commission

EU action is necessary to avoid different digital operational resilience requirements from applying to the same financial entity, when the latter operates cross-borders or undertakes different financial activities across the internal market. Also, an EU-wide oversight framework for ICT TPSPs is necessary to tackle the risks they pose to the soundness of the EU financial sector, thus complementing EU financial regulation.

Policy Context

The proposal aims at providing a sector-specific set of rules to complement the cross-sectoral Directive on measures for a high common level of cybersecurity across the Union [COM(2020) 823].

Options for Influencing the Political Process

Directorates General:	DG Financial Stability, Financial Services and Capital Markets Union
Committees of the European Parliament:	Economic and Monetary Affairs (leading), Rapporteur: Billy Kelleher (Renew Europe, Ireland)
Federal Germany Ministries:	Finance (leading)
Committees of the German Bundestag:	Finance (leading)

ASSESSMENT

Economic Impact Assessment

Financial entities have a vested interest in protecting their digital operational resilience, as failure to do so may cause significant revenue losses and reputational damage. Nevertheless, **EU requirements fostering the digital operational resilience of financial entities are justified because the products and services delivered by financial entities are** often **critical for the functioning of a society**, and the costs to society of cyber incidents targeting financial entities are particularly high. Furthermore, as financial entities are often highly interconnected, major cyber incidents at one financial entity may cause system risks for the financial sector and jeopardize financial stability.

However, the proposed **Regulation lacks proportionality and focus** in several respects. First, it is doubtful whether only financial entities that are classified as microenterprises can be regarded as non-critical for society or for financial stability considerations. A higher threshold seems more reasonable to avoid an unnecessary administrative burden. Second, the ICT risk management frameworks of financial entities do not focus on critical elements, but cover any physical components and infrastructure, premises and data centers irrespective of their relevance for the entities'

operational risk. And third, the requirements on contracts between financial entities and ICT TPSPs relate to any contract, irrespective of the criticality of the purchased ICT service. As a result, affected parties have to spend too much effort in implementing measures that do not substantially enhance their digital operational resilience.

Given the reporting costs and potential reputational damage, financial entities have few incentives to report cyber incidents. At the same time, **reports on cyber incidents** help others to identify and close security loopholes. Hence, they **produce substantial external benefits; the obligation of financial entities to report them is therefore appropriate.** However, the reporting requirements should be aligned, as far as possible, with comparable requirements imposed by other EU laws, e.g. the General Data Protection Regulation [GDPR, 2016/679] or the proposed NIS 2 Directive [COM(2020) 823, see cep**PolicyBrief**] to avoid over reporting eating up resources tackling the incident.

Financial entities increasingly make use of ICT TPSPs, e.g., for cloud computing solutions. While this offers them access to innovation and can increase their cost-efficiency, it may also increase governance, operational and lock-in risks. Currently, however, services provided by ICT TPSPs for financial entities, often do not (fully) fall within the remit of financial oversight bodies. Thus, **establishing an EU oversight framework for critical ICT TPSPs** that takes account of such new risks **may help to foster the operational resilience of the financial sector**.

Dividing supervisory tasks between EBA, ESMA and EIOPA, i.e., three supervisory bodies, raises some concern. First, it **may confront critical ICT TPSPs with different and conflicting supervisory approaches**, e.g., where their lead supervisor changes. Second, a specific ESA may lack expertise in providing adequate oversight of an ICT TPSP that provides services to a financial entity outside the ESA's usual supervisory remit. **This could be prevented by establishing a joint body of the three ESAs** thereby centralising expertise, streamlining oversight measures and creating a single point of reference for both financial entities and critical ICT TPSPs.

Furthermore, the envisaged oversight structure is not sufficiently targeted. The supervision of critical ICT TPSPs by the ESAs should focus, first, only on the services of TPSPs for financial entities excluding other sectors, and second, only on services deemed critical for financial entities. Otherwise, too many resources will be tied up by both supervisors and supervised entities, without providing any added value for strengthening digital operational resilience of the financial sector.

The ESAs' toolkit should not be restricted to recommendations, but also include direct enforcement powers vis-à-vis financial entities and critical ICT TPSPs. Without such powers, financial entities and critical ICT TPSPs will regularly be confronted with different remedial decisions taken by the competent national authorities, even where similar recommendations are made by the three ESAs. This will create inefficiencies and incoherence and may even distort competition among financial entities and critical ICT TPSPs.

The obligation on financial entities to terminate contracts with an ICT TPSP if the latter breaches applicable laws, regulations or contractual terms, or if a competent financial authority forces them to do so, is more likely to increase operational risks than dampen them, e.g., if no suitable alternative provider is swiftly available. Instead of forced contract termination, the Regulation should, as a first step, call for close coordination among the affected actors and provide at least for transition periods. Strict contract termination should only be a measure of last resort.

The restrictions on the use of critical ICT TPSPs from outside the EU are a strong interference in the freedom of contract. They may force financial entities to contract with ICT TPSPs offering less cyber secure ICT products and services, thus increasing operational risks, but also reduce choice and access to innovative ICT solutions. The Commission's targets of addressing concentration risks, in particular the high reliance of the financial sector on US cloud providers, and ensuring the EU's ability to supervise ICT TPSPs from third-countries, should be achieved by alternative means. Instead of prohibiting the use of critical ICT TPSPs from third-countries, forcing such providers to establish legal entities within the EU would be sufficient to address risks related to a potential lack of proper oversight.

Legal Assessment

Legislative Competence of the EU

The Regulation is rightly based on the internal market competence (Art. 114 TFEU).

Subsidiarity and Proportionality with Respect to Member States

Unproblematic.

Summary of the Assessment

EU requirements fostering the digital operational resilience of financial entities are justified because the products and services delivered by financial entities are critical for the functioning of a society. However, the Regulation lacks proportionality and focus. Reporting cyber incidents produces substantial external benefits. The obligation on financial entities to report them is therefore appropriate. Establishing an EU oversight framework for critical ICT TPSPs may help foster the operational resilience of the financial sector. Dividing supervisory tasks between EBA, ESMA and EIOPA may confront critical ICT TPSPs with different and conflicting supervisory approaches. This could be prevented by establishing a joint body of the three ESAs.