EUROPEAN
COMMISSION

Brussels, 24.9.2020
SWD(2020) 204 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

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} - {SEC(2020) 309 final} - {SWD(2020) 203 final}

Executive Summary Sheet

Impact assessment on Proposal for a Regulation on digital operational resilience in the financial sector

A. Need for action

Why? What is the problem being addressed?

The financial sector extensively relies on information and communication technologies (ICT). The current COVID-19 pandemic is likely to accelerate this, given the benefits in ensuring continuous remote access to financial services. Reliance on digital technologies come with concerns though; firms need to be able to withstand potential ICT disruptions so that digital incidents and threats are addressed and services maintained. In a highly interconnected financial sector that deploys cross-border vital services on which the real economy depends, vulnerabilities stemming from ICT dependence, while applicable to all economic sectors, are particularly pronounced because of (1) the deep and broad use of ICT, and (2) the potential for the effects of an operational incident at one financial firm or financial sub-sector to quickly spread to other firms or parts of the financial sector and ultimately to the rest of the economy.

Despite the financial sector being very advanced in its market and regulatory integration and thriving on a single set of harmonised rules – the EU single rulebook –, the EU response to increased operational resilience needs at both horizontal and sectorial level has been either:

- based on minimum harmonisation, thus leaving room for national interpretation and fragmentation in the single market, or
- too general and of limited application, addressing overall operational risk to a varying extent, partially regulating some components of digital operational *resilience* (e.g. ICT risk management, incident reporting and ICT third party risk) while leaving others out (testing).

EU intervention so far has not addressed operational risk in a way that corresponds to financial firms' needs to withstand, respond and recover from ICT vulnerabilities, nor does it provide financial supervisors with the tools to fulfil their mandate to contain financial instability stemming from those ICT vulnerabilities.

The current gaps and inconsistencies have led to a proliferation of uncoordinated national initiatives (e.g. on testing) and supervisory approaches (e.g. to ICT third party dependencies), which translate either in overlaps, duplications in requirements and high administrative and compliance costs for cross-border financial firms or in ICT risks remaining undetected and unaddressed. Overall, the financial sector stability and integrity are not guaranteed and the single market for financial services remains fragmented, with the consequence that consumer and investor protection are weakened.

What is this initiative expected to achieve?

The overall objective is to strengthen the digital operational resilience of the EU financial sector by streamlining and upgrading existing EU financial legislation and introducing new requirements where gaps exist, aimed at:

- improving financial firms' management of ICT risks;
- increasing supervisors' knowledge of threats and incidents;
- improving financial firms' testing of their ICT systems; and
- better overseeing risks stemming from financial firms' dependency on third party ICT providers.

More specifically, the proposal would create a more coherent and consistent incident reporting mechanisms and thus reduce administrative burdens for financial institutions and strengthen supervisory efficiency.

What is the value added of action at the EU level?

The EU single market for financial services is governed by a large body of rules set out at EU level that enables financial firms authorized in one Member State to provide services throughout the single market thanks to an EU passport. As a result, rules at national level would not be an effective way to strengthen the operational resilience of financial firms that make use of the passport. Furthermore, the EU single rulebook contains, as a result of the financial crisis, highly detailed and prescriptive rules addressing more "traditional" risks such as credit, market, counterparty and liquidity risks. The existing provisions on operational risk remain general. Strengthening digital operational resilience requires adjustments in provisions on operational risks that are already defined at EU level – and hence can only be upgraded and complemented at EU level.

B. Solutions

What legislative and non-legislative policy options have been considered? Is there a preferred choice or not? Why?

The impact assessment has considered three options, in addition to a baseline scenario of no action as regards EU financial services legislation. More specifically:

- **"Do nothing"**: rules on operational resilience would continue to be set by the current, diverging set of EU financial services provisions, partly by the NIS Directive, and by existing or future national regimes;
- **Option 1 – strengthening capital buffers**: an additional capital buffer would be introduced to increase financial firms' ability to absorb losses that could arise due to a lack of operational resilience;
- **Option 2 – a financial services digital operational resilience act**: this would introduce a comprehensive framework at EU level setting out rules on the digital operational resilience for all regulated financial institutions, that would
    - address ICT risks more comprehensively,
    - enable financial supervisors' access to information on ICT related incidents,
    - ensure that financial firms assess the effectiveness of their preventive and resilience measures and identify ICT vulnerabilities;
    - strengthen the outsourcing rules governing the indirect oversight of ICT third party providers;
    - enable a direct oversight of the activities of ICT third party providers when they provide their services to financial firms and
    - additionally, incentivise the exchange of threat intelligence in the financial sector.
- **Option 3 –resilience act combined with centralised supervision of critical third party providers**: in addition to an operational resilience act (option 2), a new authority would be created to supervise ICT third party providers of critical ICT services to financial firms. It would also more clearly delineate the financial sector from the scope of the NIS Directive.

Option 2 is the preferred choice. Compared to the other options, it is the one that achieves most of the objectives of the initiative, while taking into account the criteria of efficiency and coherence. This option also enjoys most support from the stakeholders.

Who supports which option?

Most stakeholders (private, public) agree that EU action is needed to better safeguard financial firms' operational resilience. Many also believe that EU action it is necessary to address the regulatory burdens stemming from financial firms being subject to duplicative and inconsistent rules set out in NIS, EU financial services law and national regimes (e.g. as regards incident reporting). Accordingly, few stakeholders support doing nothing. Few stakeholders see merit in safeguarding operational resilience by means of increased capital buffers (option 1). Still, this is the traditional approach to operational risk, notably in banking, and is as such considered by e.g. international standard setters. The type of qualitative measures set out in option 2 that would streamline and upgrade EU financial legislation and introduce new requirements where gaps exist while maintaining links to the horizontal NIS Directive garners broad support from stakeholders responding to the public consultation. While some stakeholders (notably public) see merit in the strengthened supervision of ICT third party providers of option 3, the creation of a new EU authority to that end only meets limited stakeholder support as does the more complete break with the NIS framework.

C. Impacts of the preferred option

What are the benefits of the preferred option (if any, otherwise main ones)?

Option 2 would address **ICT risks** across the financial sector by enhancing the capabilities of financial institutions to withstand ICT incidents. This would reduce the risk of a cyber incident quickly spreading across financial markets. While it is difficult to estimate the costs of operational incidents in the financial sector (not all incidents reported; scope of costs uncertain), industry assessments suggest that costs for the EU financial sector could range between EUR2-27bn per year. The preferred option would mitigate these direct costs and any wider impacts that major cyber incidents may have on financial stability. The elimination of overlapping **reporting requirements** would reduce administrative burdens. For example, for some the largest banks the associated savings may range between EUR40 to 100 million per year. Direct reporting would also increase supervisors' knowledge of ICT incidents. **Harmonised testing** practices would increase detection of unknown vulnerabilities and risks. It would also decrease costs, especially for cross-border firms. For example, for the 44 largest cross-border banks, total expected benefits of a common approach to testing could range between EUR11 and 88 million. By introducing a coherent set of rules on managing the risks of **third party providers of ICT services**, financial firms would have more control on how third party providers comply with the regulatory framework, which could comfort supervisors. There would also be prudential benefits stemming from supervisory oversight of ICT third party providers. Overall, the preferred option translates into broader societal benefits, stemming from a more resilient operating environment for all financial market participants and strengthened consumer and investor protection.

What are the costs of the preferred option (if any, otherwise main ones)?

The preferred option would give rise to both one-off and recurring costs. As regards the former, they are due to

investments in IT systems and are difficult to quantify given the different state of firms' legacy systems. In the absence of regulatory intervention, some financial firms have already made significant investments in ICT systems. This means that for large financial firms, implementing the measures of this proposal are likely to be low.. For smaller firms, the costs are expected to be lower as well, as they would be subject to less stringent measures proportionate to their lower risk. As regards testing, the European Supervisory Authorities have estimated that the costs related to threat-led penetration testing range between 0.1% and 0.3% of the total ICT budget of concerned firms. Costs related to incident reporting would be drastically reduced, as there would be no overlaps with the NIS reporting. Supervisors will also incur some costs, due to the additional tasks they would take on. For example, for supervisors taking part in the direct oversight of third party ICT providers, the estimated increase in FTEs could be expected in the range of 1 to 5 FTEs for the leading authority, and around 0.25 FTEs for the participating authorities.

How will businesses, SMEs and micro-enterprises be affected?

The preferred option would cover all financial firms in order to increase the operational resilience of the sector as a whole. This broad scope is important in light of the interconnected nature of the financial sector and the corresponding need to have a sound degree of overall operational resilience overall. However, when defining core requirements across the main areas of intervention, the principle of proportionality would apply both across subsectors as well as within each subsector. It would take into account, inter alia, differences in business models, size, risk profile, systemic importance, etc. For example, measures on incident reporting and testing would be less stringent for smaller financial firms.

Will there be significant impacts on national budgets and administrations?

No. The additional oversight may, as demonstrated above, require a limited degree of additional supervisory resources, which may in full or in part (if supervisory fees) be shouldered by public budgets.

Will there be other significant impacts?

The socio-economic consequences of the Covid-19 pandemic illustrate the critical nature of digital financial markets and their operational resilience. The preferred option would lay a sound base for harnessing the digital transformation by ensuring that the single market for financial services, including in the banking and the capital markets unions, is operationally resilient, based on a common set of rules and requirements that pursue security, performance, stability and a level playing field. This will also strengthen Europe's position as a financial and digital leader in the world, an objective set by the Commission in its Communication "Shaping Europe's digital future".

D. Follow up

When will the policy be reviewed?

The first review would take place three years after the entry into force of the legal instrument. The Commission would provide a report to the European Parliament and the Council on its review. The review could be supported by a public consultation, studies, expert discussions, surveys, workshops, as appropriate.