EUROPEAN COMMISSION

Brussels, 29.5.2020

SEC(2020) 307 final

REGULATORY SCRUTINY BOARD OPINION

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}
{SWD(2020)198 final}
{SWD(2020) 199 final}

EUROPEAN COMMISSION
Regulatory Scrutiny Board

Brussels,
RSB/CB, AO

Opinion

Title: **Impact assessment / Digital Operational Resilience of Financial Services**

Overall opinion: POSITIVE WITH RESERVATIONS

(A) Policy context

People trust financial institutions to keep money safe from physical and electronic theft. They also expect them to keep physical records and electronic data secure and confidential. Lax business practices, systems failures or external events must not disrupt financial services. National and EU supervisors enforce regulations that guard against these and other risks to operations.

The European Parliament has called for more attention to cyber security and ICT risks in the financial sector. EU supervisory agencies have advised about changes to legislation to improve cyber incident reporting and oversight of third party ICT service providers. They also saw a need for the EU to create a legal framework for testing resilience across the financial sector.

Current EU rules are spread across several pieces of legislation. This report assesses the case for a new EU initiative. It examines the impacts of policy options to strengthen the digital operational resilience of the EU financial sector.

(B) Summary of findings

The Board notes the useful additional information provided in advance of the meeting and commitments to make changes to the report.

However, the report still contains significant shortcomings. The Board gives a positive opinion with reservations because it expects the DG to rectify the following aspects:

(1) The report does not sufficiently focus on the political decisions to take. It does not provide enough information to judge issues of proportionality.

(2) The report does not adequately account for advice from the European supervisory agencies, or explain how and why the preferred option deviates from it.

(3) The report does not demonstrate that the preferred option is the optimal solution.

(4) The report does not adequately explain how this initiative would work together

This opinion concerns a draft impact assessment which may differ from the final version.

with parallel EU legislation that is also under revision.

(C) What to improve

(1) The report should go beyond justifying the need for action at the EU level, and explain the nature of the EU interventions that would deliver improved digital operational resilience in financial services. To this end, it should be more specific on the main components of the proposed comprehensive rules package. It should discuss whether there are alternative ways of specifying or combining sub-components. If this is the case, the report should analyse how sub-options result in different effectiveness and cost burdens. If some decisions on package components are best left to secondary legislation, the report should explain which decisions and why. It would also be useful to explain how proportionality questions would be decided.

(2) The report should better account for the 2019 joint advice of the European Supervisory Authorities on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector. The report should clarify the extent to which the options reflect this joint advice, and the grounds for deviations from it. The report should discuss the choice between responding to this advice through revisions of sectoral legislation as compared to a new cross-sectoral piece of legislation. For transparency reasons, the report could also include the former option, and possibly discard it with an explanation for doing so.

(3) The report should discuss possible differences in exposure to digital risks between financial sub-sectors in a more coherent way. It should better justify why these differences do not warrant an approach by sub-sector and how such an approach could be catered for in the preferred option.

(4) The report should explain how this initiative would be coherent with EU legislation on European Critical Infrastructure and Network and Information Systems, both of which are also under revision. The baseline might also better acknowledge the possibility of improving digital operational resilience through revisions to this legislation.

(5) The report should strengthen the explanation behind the choice of options. In particular, it should demonstrate that none of the elements of other options would perform better than the preferred option. The option comparison should present stakeholders' views on the options, including views of the supervisory authorities.

(6) On tone, the report should avoid language that appears either alarmist or advocating for a particular course of action. It should present a neutral comparison of the relative effects and costs of alternative courses of action with regard to the political decisions to take.

The Board notes the estimated costs and benefits of the preferred option in this initiative, as summarised in the attached quantification tables.

Some more technical comments have been sent directly to the author DG.

(D) Conclusion **The DG must revise the report in accordance with the Board's findings before launching the interservice consultation.** **If there are any changes in the choice or design of the preferred option in the final version of the report, the DG may need to further adjust the attached quantification tables to reflect this.**	
Full title	Digital Operational Resilience of Financial Services (DORFS) Act
Reference number	PLAN/2019/6126
Submitted to RSB on	29 April 2020
Date of RSB meeting	27 May 2020

ANNEX: Quantification tables extracted from the draft impact assessment report

The following tables contain information on the costs and benefits of the initiative on which the Board has given its opinion, as presented above.

If the draft report has been revised in line with the Board's recommendations, the content of these tables may be different from those in the final version of the impact assessment report, as published by the Commission.

I. Overview of Benefits (total for all provisions) – Preferred Option		
Description	***Amount***	***Comments***
Direct benefits		
Strengthen and harmonise requirements on ICT risk management across the EU financial sector	1. Reduce the risk of financial sector stability and integrity and effectively mitigate the negative impacts of ICT-related incidents. In order to estimate the scale of these potential negative impacts, industry estimates the cost of cyber incidents to range from USD 45 billion to USD 654 billion for the global economy in 2018. Assuming that about one fifth of incidents occur in the financial sector (see section 1.2 above), and the EU economy accounts for around 21% of the global economy, this would imply costs in the range of USD 2 billion to USD 27 billion for the EU. While a potential reduction of the negative impacts can be bigger, if we assume a conservative reduction of 10% of these risks, it would lead to benefits in the range of $200 million to $2.7 billion for the EU financial system.	*Stakeholders who benefit:* Financial institution
Enhancing and streamlining incident reporting	1. Savings from eliminating the costs of overlapping and duplicative reporting. To illustrate the scale for the banking sector, we could estimate potential savings only for the top 6 out of the more than 6000 EU banks to be in the range of up to 29 to 68 million EUR. 2. Prudential benefits for financial supervisors in the form of enhanced access to information on ICT-related incidents (due to enhancing incident reporting to cover those subsectors currently not subject to such rules).	*Stakeholders who benefit:* Financial institutions Supervisors
Promote/support voluntary information sharing	1. Increased capacity for financial institutions to leverage their collective knowledge and experience to address common threats and vulnerabilities.	*Stakeholders who benefit:* Financial institutions
Mutual acceptance of testing results across the EU financial sector	1. Cost savings from mutual acceptance of testing results performed in different jurisdictions. The costs could be estimated in the range of 250,000 to 1 million EUR per cross-border financial institution. To illustrate the scale of savings in the banking sector	*Stakeholders who benefit:* Financial institutions Supervisors

	where, according to ECB and SRB data, around 44 banking groups are undertaking cross-border activities in the EU, the total expected benefits could range between 11 and 88 million EUR.	
Strengthen the outsourcing requirements for ICT TPPs (indirect oversight)	1. Increased ability for financial institutions to enforce the contractual rights in order to ensure TPPs' compliance with the regulatory framework.	*Stakeholders who benefit:* Financial institutions
Enable tools for financial supervisors to monitor the activities of ICT TPPs (direct oversight)	1. Enhanced macro-prudential scrutiny of systemic risks resulting from the provision of service by ICT TPPs to financial institutions.	*Stakeholders who benefit:* Supervisors
Indirect benefits		
Strengthen and harmonise requirements on ICT risk management across the EU financial sector	1. Secured and resilient operating environment for all financial market participants. 2. Strengthened consumer and investor protection due to more resilient financial institutions.	*Stakeholders who benefit:* Financial institutions Consumers/investors

		II. Overview of costs – Preferred option							
		Consumers/Investors		Financial institutions		ICT TPPs		Competent authorities	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Strengthen and harmonise requirements on ICT risk management across the EU financial sector	Direct costs	NA	NA	Higher adjustment costs. Respondents to the public consultation highlighted that they are anyway planning improvements and significant investment programs in their ICT systems for the years to come. For instance, the top 4 EU banks have announced a total annual spending of around 1.1 billion EUR over the next years.	On average, costs are estimated at 10% of the IT budget on cybersecurity. In terms of revenues, this accounts on average to about 0.3% of revenues.	NA	NA	Adjust supervision to new rules. Costs associated to ICT supervision are between 5% and 10% of the total IT supervision staff.	NA
	Indirect costs	NA	Some of the cost for upgrading	NA	NA	NA	NA	NA	NA

			financial institutions' ICT systems could be passed on to their customers.						
Enhancing and streamlining incident reporting	Direct costs	NA	NA	It is estimated that on average, the costs for a big European bank for developing an internal template for incident reporting would amount to approx. €9,000. The total additional one-off costs for financial institutions is estimated in the range of €9 and €18 million.	Recurring costs for managing incidents and reporting (e.g. classification of incidents, regulatory scouting, updating templates, etc.) are estimated in the range of €18 to 36 million.	NA	NA	IT costs for the collection and management of ICT-related incident reported by financial institutions	Marginal increase in FTEs due to additional rules on incident reporting
	Indirect costs	NA	NA	NA	NA	NA	NA	NA	NA
Promote/support voluntary information sharing	Direct costs	NA	NA	Administrative costs for joining (i.e. adjustments to IT systems, legal	Annual costs may range between 1,000 EUR and 50,000 EUR, plus	NA	NA	NA	NA

				advice)	1 to 3 FTEs.				
	Indirect costs	NA	NA	NA	NA	NA	NA	NA	NA
Mutual acceptance of testing results across the EU financial sector	Direct costs	NA	NA	NA	Costs of TLPTs are in the range of 250-500.00 EUR depending on the scope, and estimated to a range between 0.1% and 0.3% of the total ICT budget. Total costs for testing the 100 financial institutions would be in the range of €25 to €50 million.	NA	NA	Adjust supervision to new rules	Marginal increase in FTEs for overseeing TLPTs and making sure it meets the requirements of the framework
	Indirect costs	NA	NA	NA	NA	NA	NA	NA	NA
Strengthen the outsourcing requirements for ICT TPPs (indirect oversight)	Direct costs	NA	NA	Adjust to new rules on outsourcing	NA	Adjust to new rules on outsourcing	NA	NA	NA
	Indirect costs	NA	NA	NA	NA	NA	NA	NA	NA
Enable tools for financial supervisors	Direct costs	NA	NA	NA	NA	Adjust to new rules of	It is estimated that	Costs for supervisory	Higher enforcement costs

to monitor the activities of ICT TPPs (direct oversight)						direct oversigh t	on average, the staffing costs for an ICT TPPs that would be subject to a direct oversig ht by financia l supervis ors would be in the range of 2 to 6 FTEs.	authoritie s participat ing in the different arrangem ents on the direct oversight of ICT TPPs could be expected in the range of 1 to 5 FTEs for the leading authority, and around 0.25 FTEs for the participat ing authoritie s.	
	Indire ct costs	NA	NA	NA	NA	NA	NA	NA	NA