Ref. Ares(2019)7834637 - 19/12/2019

European Commission

INCEPTION IMPACT ASSESSMENT

Inception Impact Assessments aim to inform citizens and stakeholders about the Commission's plans in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. Citizens and stakeholders are in particular invited to provide views on the Commission's understanding of the problem and possible solutions and to make available any relevant information that they may have, including on possible impacts of the different options.

TITLE OF THE INITIATIVE	Regulation on Digital Operational Resilience for the Financial Sectors
LEAD DG (RESPONSIBLE UNIT)	FISMA - Unit D2
LIKELY TYPE OF INITIATIVE	Legislative proposal
INDICATIVE PLANNING	2020
ADDITIONAL INFORMATION	–

The Inception Impact Assessment is provided for information purposes only. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content. All elements of the initiative described by the Inception impact assessment, including its timing, are subject to change.

A. Context, Problem definition and Subsidiarity Check

Context [max 10 lines]

The financial sector is the largest user of Information and Communication Technology (ICT) infrastructure in the world, accounting for about a fifth of all IT expenditure. This dependence will further increase with the growing use of emerging models, concepts or technologies, as evidenced by financial services benefitting more and more from the use of distributed ledger and artificial intelligence. Accordingly, whether we talk about online banking and insurance services, mobile payment applications, digital trading platforms, high frequency trading algorithms, digital clearing and settlement systems, most financial services delivered today rely on digital technologies and data.

Dependence on ICT and data raises new challenges in terms of operational resilience. The increasing level of digitalisation of financial services coupled with the presence of high value assets and data make the financial system vulnerable to operational incidents and cyber-attacks. According to a European Parliament report[1], the financial sector is three times more at risk of being the target of cyber-attacks than any other economic sector. In the recent years, the frequency and impact of cyber incidents has been increasing, with research estimating the total cost to amount to several billions for the global economy.

The Network and Information Security (NIS) Directive[2] provides general requirements for the security of network and information systems across sectors, including for some operators in the financial sector. At the same time, as part of their broader mandate to ensure the operational resilience of financial firms, financial supervisors, tasked with ensuring the stability and integrity of the financial system, are increasingly requiring financial institutions to effectively manage operational resilience capabilities, in particular to address ICT and security risks to mitigate any negative impact on financial stability and market integrity. International financial standard setters have developed, or are working on standards and principles governing these activities.

The EU financial sector is governed by a detailed and fully harmonised single rulebook, ensuring proper regulation and a level playing field across the single market, which in some areas forms the basis for EU bodies to supervise specific financial institutions (e.g. Single Supervisory Mechanism (SSM) supervision of credit institutions). ICT risk is one of the major components of operational risk, which our prudential supervisors continuously assess and monitor as part of their mandate. In order to preserve and build on this harmonised approach and implement international standards with a view to more effectively address operational resilience and in particular the ICT risks in the financial sector, it is essential that financial supervisors work in a harmonised and convergent manner across Member States and across different parts of the financial sector. Where EU bodies have direct supervisory responsibilities over certain financial institutions, this will also ensure that they have the necessary and

[1] Available here: http://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.pdf

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

appropriately framed powers.

In April 2019, in response to the Fintech Action Plan, the European Supervisory Authorities (ESAs) provided technical advice[3] to the Commission on the need for legislative improvements on ICT risk management requirements and on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector.

Problem the initiative aims to tackle [max 20 lines]

The reform that followed the financial crisis primarily strengthened the financial resilience of the EU financial sector, increasing its competitiveness and stability from economic, prudential and market conduct perspectives. The operational resilience of our financial sector, including its digital dimension (in particular ICT and security risks) have been less in the focus of the post-crisis regulatory reform, but have nonetheless continued to grow as emerging challenges for the financial sector in recent years.

The EU financial services regulatory landscape does include operational resilience provisions also touching the ICT and security risk components, in particular for financial market infrastructures, which apply in this respect rules by far more demanding than those laid down in the NIS Directive. However, in other parts of the financial sector acquis, rules on ICT and security risk are more general or even inexistent. Overall, the existing provisions are not consistently addressed across the financial acquis and appear fragmented in terms of scope, granularity and specificity, as evidenced by the European Supervisory Authorities in their technical advice.[4] These requirements should be upgraded, streamlined and harmonised at EU level in order to strengthen the EU single rulebook. In addition, the goal of the proposed legislative initiative is also to frame and streamline financial supervisors' (e.g. SSM, ESAs, etc.) set of supervisory / monitoring tools (e.g. access to ICT and security incident notifications, overview of third party risks, etc.). Harmonised powers enable an effective monitoring of compliance by regulated financial entities with (increased) operational resilience provisions. The initiative also aims at resolving the EU financial sector disparities and gaps in terms of ICT security among operational resilience requirements. Such disparities or lacunae risk undermining the unity of the EU single rulebook, the level playing field and security. They relate in particular to:

- **Heterogeneity and disparity of ICT security among operational resilience requirements across the EU financial services legislation** – the current EU financial services acquis appears fragmented in the level of detail and specificity of ICT and security risk provisions. Financial market participants of certain sectors are subject to more specific requirements (e.g. under PSD2, CSDR, EMIR, etc.),[5] while, for others, provisions are either too general or even inexistent (e.g. CRDIV/CRR, Solvency II, UCITS/AIFMD, etc.).[6] The NIS Directive also provides general provisions for the security of network and information systems of some operators in the financial sector - e.g. credit institutions, central counterparty clearing (CCPs) and trading venues - which are partly disabled by the *lex specialis* clause.
- **Absence of requirements or a multiplication of obligations on the reporting of the same ICT incident to different authorities** – the EU financial services legislation includes specific obligations to notify ICT and/or operational incidents to supervisory authorities (e.g. PSD2 and CSDR), but these obligations differ from each other. Other pieces of the financial legislation remain silent, leading to various supervisors setting up their own reporting systems. The NIS Directive also requires some operators in the financial sector (e.g. credit institutions, CCPs and trading venues) to notify incidents to the NIS authority, - which in some Member States is the prudential authority, while in others is an authority with no regulatory or supervisory mandate over the financial sector. This results in an incomplete supervisory overview of the frequency of occurrence and significance of ICT and security incidents while at the same time presenting financial institutions with complex and potentially inconsistent reporting requirements. The lack of information on significant ICT and security incidents also reduces the capability to assess and monitor risks that may affect the stability of the financial system.
- **A diversity of digital operational resilience testing frameworks** (e.g. threat led penetration testing - TLPT) – a number of Member States and supervisors have developed and/or are in the process of implementing digital operational resilience testing frameworks which present similarities but also differences in terms of scope, testing modalities and requirements or authorities involved. Uncoordinated testing has the potential to segment the Single Market and undermine the single supervisory approach. At the same time, the lack of cross-border acceptance of test results among the supervisory authorities is

[3] Available here: https://esas-joint-committee.europa.eu/Pages/News/ESAs-publish-Joint-Advice-on-Information-and-Communication-Technology-risk-management-and-cybersecurity.aspx

[4] Idem.

[5] The Payment Services Directive 2 (PSD2) - Directive (EU) 2015/2366, the Central Securities Depositories Regulation (CSDR) - Regulation (EU) No 909/2014, the European Market Infrastructure Regulation (EMIR) - Regulation (EU) No 648/2012.

[6] The Capital Requirements Directive (CRD IV) - Directive 2013/36/EU, the Capital Requirements Regulation (CRR) - Regulation (EU) No 575/2013, Solvency II Directive - Directive 2009/138/EC, The Undertakings for Collective Investment in Transferable Securities Directive (UCITS) - Directive 2009/65/EC, The Alternative Investment Fund Managers Directive (AIFMD) - Directive 2011/61/EU.

generating additional burden and costs.

- **Lack of coherent oversight over the activities of third party providers to financial sector entities** – financial sector entities are increasingly making use of (ICT) third party providers. Operational, amongst which ICT and security incidents occurring at third-party service providers may result in temporary outages affecting financial institutions. Contractual limitations stemming from agreements between financial institutions and ICT third party providers may impair the ability of financial institutions to assess whether the service is being delivered in line with the financial regulatory framework. Currently, there is no EU wide coherent oversight framework to enable an effective monitoring by the financial supervisory authorities of the activities of such (ICT) third party providers in relation to the services they offer to financial actors.

  Financial institutions are sometimes confronted with supervisory hesitations when seeking to contract tasks to third parties, as supervisors have either insufficient insight into whether such third parties present risks or may not always possess all needed tools to analyse and oversee the impact of such third party dependencies. In other instances, supervisors are imposing diverging requirements on these financial institutions. For some ICT products or services, a limited number of ICT third party providers dominate the market. This may lead to supervisory and regulatory concerns around the level of third party dependencies, and concentration and contagion risks, which may ultimately undermine the stability of the EU financial system.

Basis for EU intervention (legal basis and subsidiarity check) [max 10 lines]

The Treaty on the Functioning of the European Union confers upon the European institutions the competence to lay down appropriate provisions that have as their object the establishment and functioning of the internal market (Article 114 TFEU). However, other suitable legal bases could be also explored, for instance Article 53 (1) TFEU.

This competence encompasses the power of enacting legislation at EU level addressing a series of prudential, market conduct and other relevant requirements for entities operating in the financial sector and for their supervisors. As financial services are currently – and even more so in the future - overwhelmingly deployed through varied and complex ICT-based systems and processes, there is a clear need that all financial actors understand and remain at all times in full control over the (ICT) security and operational risks deriving from their use of technological means.

However, the way that ICT security and operational resilience requirements are addressed at EU level is rather incomplete and fragmented. Moreover, an unscrutinised use of (ICT) third-party providers - especially the ones that are critical for the financial entities' daily operations and functions - may pose risks to the financial stability of the Union.

The ESAs joint technical advice shows that Member States generally welcome further legislative improvements on ICT and security risk management (as well as on governance-related aspects) that build on existing provisions in the EU financial services legislation and the work of international standard setters.

The envisaged rules should avoid unnecessary burden, regulatory disparities and ensure a level playing field for all entities operating or providing services to the financial sector.

The objectives of the initiative (see the section below) can be better achieved at the EU level, rather than by the Member States alone, in view of:

- The cross-border dimension of ICT risks / security threats among operational resilience challenges.
- The fact that financial institutions operate across borders in several Member States and also rely on service providers and infrastructures located across the EU.
- Only harmonised EU action could reduce the reporting burden - and the implicit costs - of the same ICT and security incidents to different EU and/or national authorities.
- EU action is needed to facilitate the mutual recognition/acceptance of the testing results of entities operating cross-border that are subject to different TLPTs in different Member States.
- The lack of an appropriate oversight framework to monitor the risks stemming from (ICT) third party providers, including concentration and contagion risks at EU level.

In accordance with the principle of proportionality, the proposed rules will not go beyond what is necessary in order to achieve the objectives. The initiative will address those aspects that Member States cannot achieve on their own and where the costs are commensurate with the objective to be achieved.

B. Objectives and Policy options [max 20 lines]

The overall objective of the initiative is to strengthen the digital operational resilience of the EU financial sector entities, including their ICT security, by streamlining and upgrading existing rules and introducing requirements where gaps exist, duly taking into account recommendations endorsed at international level, as well as existing EU and national frameworks on ICT and security risk management. This initiative is without prejudice to the data

breach notification laid down in the General Data Protection Regulation (GDPR). Thus, the rules concerning the data breach notification laid down in the GDPR are not within the scope of this Inception Impact Assessment.

At this preliminary stage of reflection, the Commission is considering several possible policy options to achieve the pursued general objective. Under a baseline scenario, the ICT and security risks under operational resilience rules for financial services would continue to be set by current disparate provisions in the EU financial services legislation and partly by the NIS Directive.

On that basis, among the policy options to be considered are targeted amendments to EU financial services legislation (while the possible revision of the NIS Directive may bring along the opportunity to revisit its scope and the depth of its substantive requirements) and a general yet bespoke legal framework addressing the digital operational resilience for all regulated financial entities, applying across the different financial sectors taking into account, where relevant, specific needs arising for financial services sectors.

C. Preliminary Assessment of Expected Impacts [max 20 lines]

Likely economic impacts

The initiative will have a positive impact on the functioning of the internal market by virtue of:

- strengthening the level of protection to address ICT and security risks (in the context of the operational resilience of financial sector entities);
- ultimately increasing customer protection;
- strengthening the Single rulebook and thus the consistency of regulatory and supervisory requirements.

By reducing the level and magnitude of technological disruptions, the initiative would help reduce operational risks which may pose threats to the financial stability and market integrity of the EU financial sector.

In addition, by stimulating the use of ICT-resilient technologies, processes and services in the financial sector, the initiative will boost the growth potential of the digital economy in the Union thus translating into additional economic growth in Europe.

The initiative will contribute to bringing further investment in the ICT security market. The growth of the ICT and security threat intelligence sharing and the promotion of threat led penetration-testing will enable varied business solutions, open up new revenue streams, drive efficiencies and improve the supply and demand side of existing threat intelligence and penetration testing services. It will allow a more secure and eased deployment of new and innovative technological applications and systems.

The initiative will also contribute to facilitating further development of an ICT and security risk insurance market in Europe by mandating the reporting of ICT and security incidents, which in turn will allow the development of adequate pricing and risk management models by insurance companies.

Finally, supervisors will have a more appropriate regulatory framework to carry out an oversight of activities of (ICT) third party providers to the financial sector. A more tailored set of risk assessment and monitoring tools would help supervisors perform their role in a more targeted, coherent and efficient way, enhancing the orderly and effective functioning of financial markets and reducing the risk to financial stability.

The likely economic impacts of the various options will be analysed in more detail in the Impact Assessment.

Likely social impacts

By strengthening the ICT security component of the operational resilience of EU financial institutions, customers will be better protected from the risks incurred by these firms.

Likely environmental impacts

By strengthening the ICT security and operational resilience of financial institutions, the initiative would promote an enhanced use of the latest generation ICT infrastructures and services, which are environmentally more sustainable. Replacing inefficient or insecure legacy infrastructures would contribute to a decrease in the number of costly ICT and security incidents, thus also freeing up resources and making them available for sustainable investments.

Likely impacts on fundamental rights

Strengthening the ICT security component of the operational resilience of the EU financial institutions would likely increase the level of protection in respect to customers' personal data +that financial institutions deal with and hold.

The possible impact of the initiative on mitigating or better managing the risk of data breaches (affecting the personal data of individual customers) would also be part of the analysis without prejudice to the data breach notification rules laid down in the General Data Protection Regulation (GDPR).

Likely impacts on simplification and/or administrative burden

Streamlining the existing regulatory framework including the reporting of ICT and security incidents would result in a reduction of administrative burdens and compliance costs for financial institutions currently reporting the same ICT and security incident to different authorities.

In addition, enabling mutual acceptance of testing results for cross-border entities would result in less compliance costs.

D. Evidence Base, Data collection and Better Regulation Instruments

Impact assessment

An impact assessment is being prepared to support the preparation of this initiative and to inform the Commission's decision.

Evidence base and data collection [max 10 lines]

In April 2019, the Commission received two joint technical advices from the European Supervisory Authorities that provide qualitative and quantitative evidence in support of comprehensive action at EU level on legislative improvements in the area of ICT and security risk management and governance.

In line with the general principles in the Better Regulation guidelines on the need for evidence based impact assessment, the Commission will collect evidence through several sources that include:

- Publicly available reports, studies, surveys, position papers and other relevant documents drawn up by stakeholders.
- Data from the series of Eurobarometers on Cybersecurity.[7]
- Input from workshops, bilateral meetings and consultation with Member States, supervisors and industry stakeholders.
- The results of the public consultation targeting all interested parties, which will be launched in December 2019.

The Commission is also considering input received previously in the Call for Evidence[8] on the efficiency, consistency and coherence of the overall EU regulatory framework for financial services, as well as in the public consultation on FinTech,[9] where several respondents pointed to various issues relevant for the initiative.

Consultation of citizens and stakeholders [max 10 lines]

The consultation strategy will consist of a mix of open consultation, targeted meetings and workshops to gather views on key aspects of the proposal, such as an oversight of (ICT) third party providers, a digital operational resilience testing framework, ICT and security incident reporting rules and ICT and security risk management framework, as well as any potential costs that may be estimated.

The public consultation will target all stakeholders (EU citizens, Member States, ESAs, NCAs, financial institutions, crypto-asset service provider, investors etc.). It will be open for 13 weeks and be published on the Have your Say portal. As subsequent steps in the broader consultation process, targeted workshops with national authorities and industry stakeholders across the different financial subsectors - e.g. banks, (re)insurance companies, investment firms, central securities depositories, asset managers, etc. - will be organised in 2020. These aim at providing further evidence and views on the proposal(s) and confirm the magnitude of the problem, costs associated with certain options as well as potential economic impacts.

Finally, the Commission will also consult the Expert Group on Banking, Payments and Insurance (EGBPI) and the Financial Services Users Group (FSUG), and will continue to liaise with stakeholders through bilateral ad-hoc contacts to help further substantiate the analysis of the available policy options in line with the Better Regulation guidelines.

Will an Implementation plan be established? [max 5 lines]

If the new rules take the form of a directive, an implementation plan will be established.

[7] Available here: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/index#p=1&instruments=SPECIAL&yearFrom=1974&yearTo=2018&search=cyber

[8] Available here: http://ec.europa.eu/finance/consultations/2015/financial-regulatory-framework-review/index_en.htm

[9] Available here: https://ec.europa.eu/info/consultations/finance-2017-fintech_en