EUROPEAN
COMMISSION

Brussels, 24.9.2020
SWD(2020) 198 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

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} - {SEC(2020) 307 final} - {SWD(2020) 199 final}

TABLE OF CONTENTS

1. INTRODUCTION 3
   1.1. Political context 3
   1.2. Market context 5
2. PROBLEM DEFINITION AND SUBSIDIARITY 10
   2.1. Problem definition 10
      2.1.1. Fragmentation in managing ICT risks 10
      2.1.2. Ineffective reporting of and limited awareness about threats and incidents 12
      2.1.3. Limited and uncoordinated testing 15
      2.1.4. ICT third-party risks 17
      Problem tree 22
   2.2. The EU's need to act and justification 23
      2.2.1. Legal basis 23
      2.2.2. Subsidiarity: Need for EU action 23
      2.2.3. Subsidiarity: Added value of EU action 24
3. OBJECTIVES 25
      Table 2 – Intervention logic diagram 26
4. OPTIONS AND ASSESSMENT OF POLICY OPTIONS 27
   4.1. Do nothing: No change in the EU financial services regulatory framework 29
      4.1.1. Overall assessment of the current state of play and expected impact 30
   4.2. Option 1: Strengthening financial institutions' ability to absorb losses stemming from lack of digital operational resilience 33
      4.2.1. Assessment of the impact 34
      4.2.2. Overall assessment of the option 36
   4.3. Option 2: A digital operational resilience act for the financial sector 37
      4.3.1. Assessment of the impact 40
      4.3.2. Overall assessment of the option 45
   4.4. Option 3: A financial services digital operational resilience act together with centralised supervision of activities of critical ICT TPPs 46
      4.4.1. Assessment of the impact 47
      4.4.2. Overall assessment of the option 48
   4.5. Comparison of options 50
   4.6. Retained option 51
5. OTHER SPECIFIC IMPACTS OF THE RETAINED POLICY OPTION 52
   5.1. Impacts on SMEs 52
   5.2. Social impacts 52
   5.3. Environmental impacts 53

6. MONITORING AND EVALUATION 53
ANNEX 1 – PROCEDURAL INFORMATION 55
1. Lead DG, Decide planning / CWP references 55
2. Organisation and timing 55
3. Consultation of the Regulatory Scrutiny Board (RSB) 55
4. Evidence, sources and quality 56
ANNEX 2 – OVERVIEW OF THE REGULATORY FRAMEWORK CONCERNING DIGITAL OPERATIONAL RESILIENCE 57
1. ICT risk management 57
2. Incident notification 62
3. Testing 63
4. Third party risk 64
ANNEX 3 – SYNOPIS REPORT ON STAKEHOLDER CONSULTATIONS 67
1. Introduction 67
2. Overview of respondents and responses 68
3. Summary of respondents' feedback 69
3.1. ICT risk management requirements 69
3.2. ICT incident reporting requirements 72
3.3. Digital operational resilience testing 73
3.4. Addressing third party risk: oversight of TPPs (including outsourcing) 75
3.5. Other areas where EU action may be needed 79
3.6. Interaction with the NIS Directive 81
3.7. Potential impacts 83
ANNEX 4 – DETAILED PROVISIONS UNDER THE RETAINED OPTION 86
ANNEX 5 – WHO IS AFFECTED BY THE INITIATIVE AND HOW? 89
1. Practical implications of the initiative 89
2. Summary of cost and benefits 89
ANNEX 6 – GLOSSARY 95

1. INTRODUCTION

1.1. Political context

As stated by President von der Leyen in her Political Guidelines,[1] and set out in the Communication 'Shaping Europe's digital future',[2] it is crucial that Europe can reap all the benefits of the digital age and strengthens its industry and innovation capacity, within safe and ethical boundaries. The *European strategy for data*[3] sets out four pillars – data protection, fundamental rights, safety and cyber-security – as essential pre-requisites for a society empowered by data.

New technologies are transforming the EU financial system and the way it provides services to Europe's businesses and citizens. The socioeconomic consequences of the Covid-19 pandemic have also highlighted the importance of digital finance and the imperative of allowing business to be conducted remotely and through innovative digital technologies, wherever possible.

Digitalisation and operational resilience in the financial sector are two sides of the same coin, as digital opportunities can also give rise to risks that need to be well understood and managed. It is of paramount importance for financial institutions to assure business continuity, confidence and the provision of services to consumers and the economy, both under normal operating conditions, and in particular under situations of stress (see Box 1 for further explanation on the concept of operational resilience). This is amply demonstrated by the operational challenges resulting from Covid-19 response measures. The Financial Stability Board (FSB) has also warned that the financial industry is at particular risk of cyber-attack during the Covid-19 outbreak given the increase in remote working,[4] where continuity in delivering some products and services is ensured by employees working from home. Industry reports[5] also highlight several other implications for financial institutions in this context, such as the large-scale shift to remote working and digital channels in a very short period of time, which led to higher demands on institutions' digital infrastructure to replace manual operations, increased use of third party service providers (e.g. cloud service providers), employees working with sensitive data in less secure home-based environments, increased demand for quick and tailored crisis communication channels with all stakeholders (e.g. employees, customers, regulators), etc.

In recent years, and because ICT risks know no borders, ICT risks have come onto the radar of national, European and international policy makers, regulators and standard-setting bodies in an attempt to enhance resilience, set standards and coordinate regulatory or supervisory work. This work has been carried out both across industries and in a sector specific manner for a number of sectors, including financial services. In the financial sector, the European Systemic Risk Board (ESRB) identified cyber risk as a source of systemic risk to the EU

[1] Ursula Von Der Leyen, Political Guidelines for the next European Commission, 2019-2024.
[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, Shaping Europe's Digital Future, COM(2020) 67 final.
[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, A European strategy for data, COM(2020) 66 final.
[4] Financial Stability Board (FSB), *COVID-19 pandemic: Financial stability implications and policy measures taken* (15 April 2020), https://www.fsb.org/wp-content/uploads/P150420.pdf
[5] See https://www2.deloitte.com/us/en/insights/economy/covid-19/banking-and-capital-markets-impact-covid-19.html?id=us:2em:3pa:financial-services:eng:di:031720, https://home.kpmg/xx/en/home/insights/2020/04/covid-19-insights-emerging-risks.html, and https://www.cnbctv18.com/technology/mcafee-report-shows-rise-in-cyber-attacks-as-cloud-services-use-goes-up-during-covid-19-6013631.htm

financial system, with the potential to have serious negative consequences for the real economy.[6] The FSB has also stressed that risks to financial stability could arise from "interconnected IT systems between multiple financial institutions or between financial institutions and third-party service providers".[7] At international level, the Basel Committee on Banking Supervision[8] (BCBS), Committee on Payments and Markets Infrastructures[9] (CPMI), Financial Stability Board[10] (FSB), Financial Stability Institute[11] (FSI), G7[12] and G20 all aim to provide authorities and market operators across jurisdictions with tools to bolster the resilience of their financial systems.

Despite the significant progress made through national and European targeted policy and legislative initiatives, ICT risks continue to pose a challenge to the operational resilience, performance and the stability of the EU financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience[13] of the EU financial sector and aimed at safeguarding EU competitiveness and stability from economic, prudential and market conduct perspectives. ICT security and overall digital operational resilience are part of operational risk, but have been less in the focus of the post-crisis regulatory agenda, and have developed only in some areas of EU financial markets policy and regulation, or only in a few Member States. The Commission's 2018 Fintech action plan highlighted that making the EU financial sector more resilient also from an operational perspective is of paramount importance to ensure that it is well protected, that it can recover from breaches and incidents, that it is functioning well and that financial services are delivered effectively and smoothly across the EU, including under situations of stress, and that consumer and market trust and confidence are preserved.[14]

As the EU financial sector is highly integrated and interconnected, so is EU level regulation and supervision. To maintain a level playing field among financial institutions and to ensure that they are all subject to a high level of prudential, market integrity and market conduct rules, an EU system of financial supervision and a Single Rulebook for financial services[15] has been gradually created, including the creation of EU supervisory authorities (ESAs) for banking (EBA), securities markets (ESMA), insurance and occupational pensions (EIOPA), the Single Supervisory Mechanism (SSM) at the ECB and the Single Resolution Board (SRB). This level of regulatory and supervisory integration at EU level is unique and unmatched in other sectors.

---

[6] ESRB report *Systemic Cyber Risk* from February 2020, https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html.
[7] https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document/
[8] Basel Committee on Banking Supervision, *Cyber-resilience: Range of practices*, December 2018.
[9] The Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO) *Guidance on cyber resilience for financial market infrastructures* (2016).
[10] The FSB *Cyber Lexicon* (2018), and also a *Cyber Incident Response and Recovery: Progress Report to the G20 Finance Ministers and Central Bank Governors meeting in Fukuoka, 8-9 June 2019*, May 2019.
[11] The Financial Stability Institute *Regulatory approaches to enhance banks' cyber security frameworks* (2017).
[12] The G7 *Fundamental Elements of Cybersecurity for the Financial Sector* (2016), the *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* (2018) and the *Fundamental Elements for Threat-led Penetration Testing* (2019). Besides, the G7 has started conducting cross-jurisdictional cyber exercises.
[13] The different measures adopted aimed to increase the capital position, liquidity, reduce market and credit risk for financial institutions, etc.
[14] European Commission, *Fintech Action Plan*, COM/2018/0109 final.
[15] The Single Rulebook represents the harmonised prudential rules that EU financial institutions must abide to. The term Single Rulebook was coined in 2009 by the European Council to refer to the objective to unify the EU regulatory framework to complete the single market in financial services.

Nonetheless, the European Single Rulebook for financial services and the European system of financial supervision does not comprehensively harmonise provisions tackling digital operational resilience and ICT security. Digital operational resilience and security are essential for financial markets, especially in the digital age, and no less important than for example common prudential or market conduct standard; the financial services Single Rulebook and system of supervision should therefore be developed to cover this field too.

In April 2019, the ESAs therefore jointly issued two pieces of technical advice emphasising the need for a coherent approach to ICT risk in finance, recommending to strengthen, in a proportionate way, the digital operational resilience of the financial services industry through an EU sector-specific initiative.[16]

The purpose of this document is to assess the case for action, the objectives, and the impact of different policy options for a legislative initiative on digital operational resilience in the Financial Sector, as envisaged by the 2020 Commission work programme. [17]

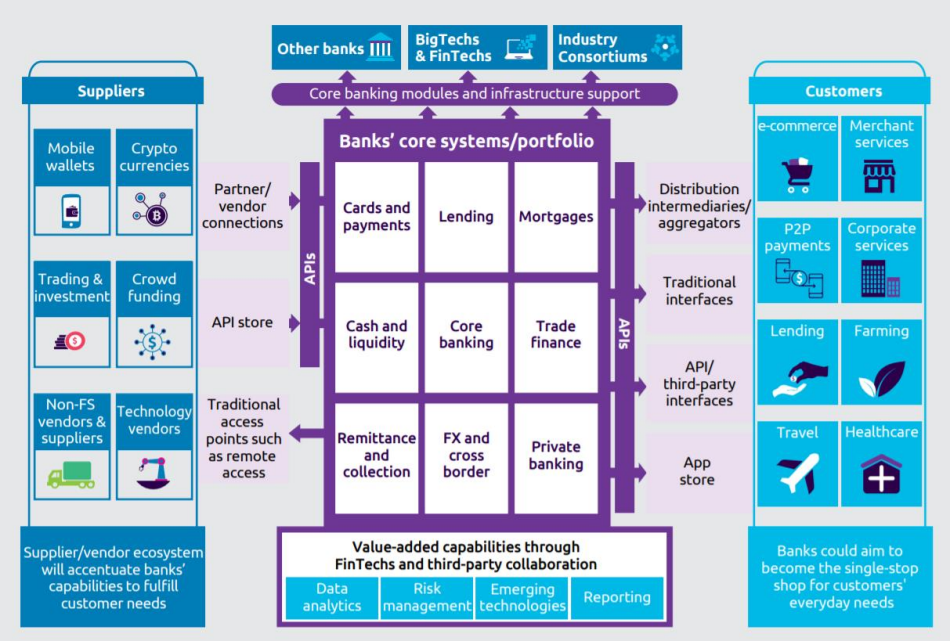
1.2. Market context

The past decades have witnessed significant advances and increased complexity in the use of ICT in finance. The financial sector has become as much about data and technology as it is about money and capital. In terms of expenditure, the financial sector is by quite some distance the largest ICT sector of the economy, accounting for about 20% of global ICT expenditure.[18]

Digitalization is a vital driving force in the transformation of nearly all financial sectors. It this not only covers payments, which increasingly have moved from cash and paper-based methods to digital solutions, but also back-office operations, electronic and algorithmic trading, lending and funding including credit rating, insurance underwriting, claim management and peer-to-peer finance. According to a report by the Bank for International settlements,[19] which reflects numbers from 2016, around 90% of all futures trading was done electronically, and 80% of all foreign currency exchange and equity trading. Other industry reports[20] show that around 70% of Europeans use online banking on a regular basis, with this percentage going above 90% in some Member States. ICT risk therefore puts a continuous stress on the financial sector due the sector's overwhelming dependency on software, data and digital processes for performing key financial services operations and functions. Figure 1 illustrates the depth and breadth of digitalisation in one financial sector (banking).

[16] Joint Advice of the European Supervisory Authorities, *To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector*, JC 2019 26 (2019).
[17] https://ec.europa.eu/info/publications/2020-commission-work-programme-key-documents_en.
[18] *IT spending worldwide by vertical industry in 2014 and 2015*, Statista. According to Statista, the financial sector combined IT spending worldwide in 2014 and 2015 amounted to US$ 699 billion, well ahead of manufacturing and natural resources (US$ 477 bn), media (US$ 429 bn) or governments (US$ 425 bn). Total global IT spending in 2014 and 2015 were estimated at US$ 3734 billion and US$ 3509 billion respectively, suggesting that almost 1 in every 5 US$ spent on IT worldwide is in the financial sector.
[19] https://www.bis.org/publ/mktc07.pdf
[20] https://money-gate.com/europeans-top-online-banks/.

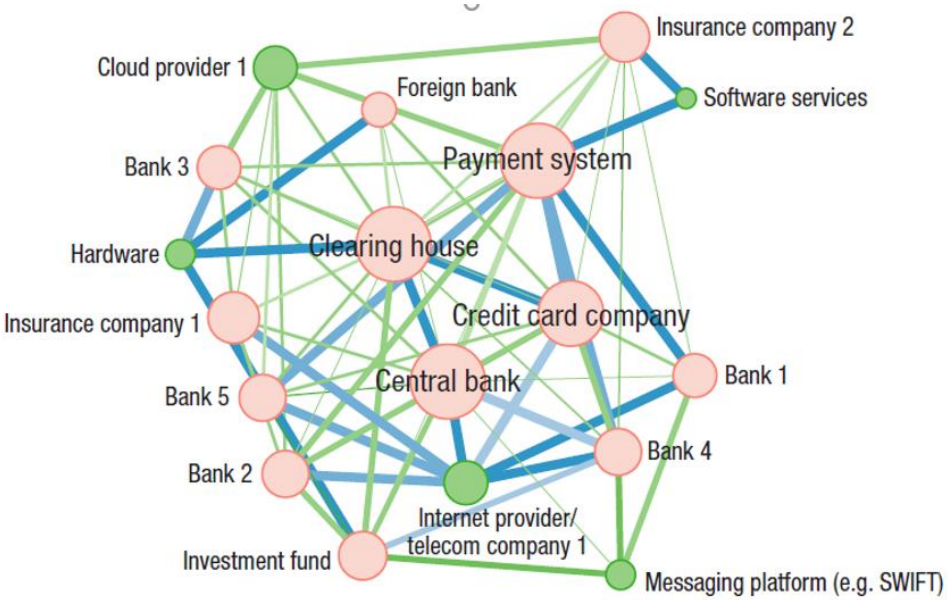
Figure 1. Bank in an open ecosystem context



Source: Capgemini, World Payments Report, 2019[21]

Finance has not only become largely digital throughout the whole sector, but digitalisation has also deepened interconnections and dependencies within the financial sector and with infrastructure and service providers (see figure 2). According to ECB, almost 100 bn payment transactions took place in 2018[22] and about 500 million securities transactions take place every year.[23]

Figure 2. Stylised interconnectedness in the financial sector



[21] https://www.europeanpaymentscouncil.eu/sites/default/files/inline-files/World-Payments-Report-2019.pdf.
[22] https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2018~c758d7e773.en.html.
[23] https://www.ecb.europa.eu/stats/payment_statistics/securities/html/index.en.html.

Source: IMF, Cybersecurity Risk Supervision, 2019[24]

Box 1 – basic concepts

ICT risks are generally understood to mean risks arising with the use of network and information systems or communication technology. That includes malfunctions, hardware and software failures, disruptions caused by human error, spam, viruses etc., misuses or other types of adverse malicious and non-malicious events that can compromise the security and resilience of such network information systems or communications technologies, the operation and running of processes or the provision of services. For example, major losses are incurred when data or ICT systems lose integrity or become unavailable, confidential data is breached or physical ICT infrastructure is damaged.

ICT risk management is used to describe the application of risk management processes and mechanisms to information and communication technologies in order to manage operational risk of a digital nature. Every firm, in the financial sector and outside, should identify risks to its ICT systems and data in order to reduce or manage those risks and develop a response plan in the event of a crisis.

Digital operational resilience refers to the *qualitative* processes that a financial institution undergoes to build, maintain and review, on a continuous basis, the full operational integrity of its ICT systems, for a safe and compliant running of its operations and deployment of services. Digital operational resilience complements the approach embedded in existing financial services regulation to address financial institutions' operational risk, which has so far relied mainly on identifying, monitoring and addressing risks through *quantitative* approaches (in particular an effective capital planning and provisioning to cover for possible losses stemming from those risks).

Digital operational resilience requires the activation of a set of comprehensive functions, policies, processes of ICT risk management that allow the financial institution to be prepared to protect its ICT systems and prevent disruptions, to adapt to changing ICT patterns and to recover from those disruptions (within certain limits of tolerance either acceptable or known in advance). Digital operational resilience requirements thus address both the institution's internal organisation processes and its inherent technological dependencies to third parties for the deployment of ICT supporting business functions – in particular in relation to the monitoring of the digital risks posed by third parties through outsourcing arrangements.

For a financial institution to be able to achieve full operational integrity on an ongoing basis, its digital operational resilience must be the consequent result of a synergy of distinct components: corporate governance requirements, a defined detailed ICT risk management framework (including incident reporting and testing), a comprehensive monitoring of digital risk coming from third party dependencies (in particular from outsourcing), as well as mechanisms for coordination between financial institutions and with financial supervisors.

While being a broader concept, the digital operational resilience fully integrates and relies on the concept of "*security of network and information systems*" which is vital to ensure a safe and compliant use of any of the financial institution's technology or data dependent components, tools and processes to support its business. The horizontal

[24] https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/23/Cybersecurity-Risk-Supervision-46238.

framework on cybersecurity, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS) defines the "security of network and information systems" in Article 4(2) as *the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information system.*

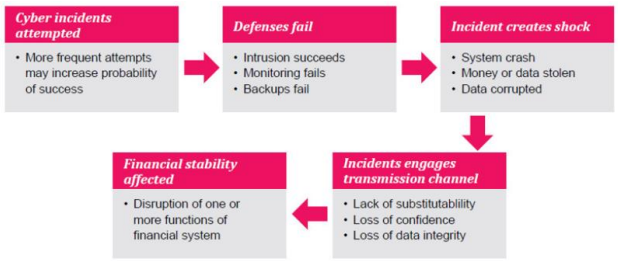
Firms operating in the financial services industry are 300 times as likely as other companies to be the target of cyber-attacks.[25] This was also acknowledged in a European Parliament report.[26]

Despite significant investment in ICT security technology, the average cost to financial institutions resulting from operational incidents keeps on increasing. From 2013 to 2018, the total annual cost of all types of cyberattacks increased by 72%. An 2018 IMF modelling exercise put the base-case average aggregated annual loss due to cyber-attacks at 9% of banks' net income globally, or around $100 billion. In a severe scenario — in which the frequency of cyber-attacks is twice as high as in the past due to greater contagion — losses could be 2½–3½ times as high as this, or $270 billion to $350 billion.[27]

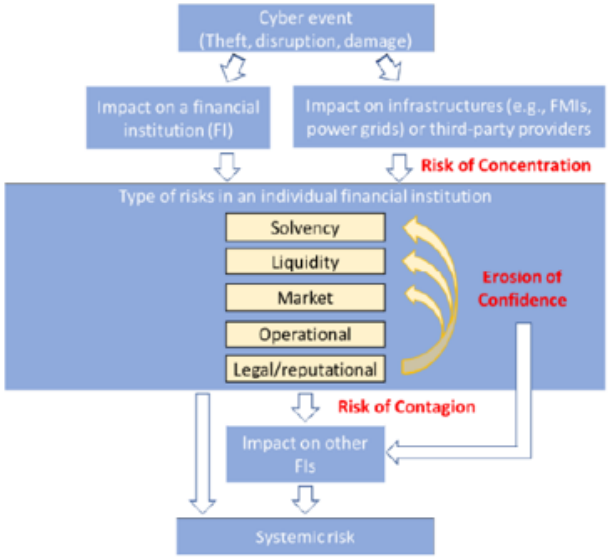
ICT security breaches affecting a market participant in the financial sector are prone to spread within the financial system, as its participants have numerous and very close interconnections. According to the ESRB,[28] the high level of interconnectedness across financial institutions, financial markets and financial market infrastructures, and particularly the interdependencies of their IT systems, constitute a potential vulnerability as a localised cyber incident could quickly spread across markets and jurisdictions. For example, ICT systems underpinning payment operations link together thousands of credit institutions both to each other and with payment services providers. Securities trading and settlement chains bring together credit institutions, investment firms, trading venues, central securities depositories and central counterparties. ICT security breaches in the financial sector therefore affect not just a single financial entity or sector and its customers, but adversely impact the stability of the whole financial system. As a result, a localised ICT threat or incident could more likely propagate at a faster pace from any of the ca. 21 000 single financial institutions in Europe towards the entire financial system, unhindered by any geographical boundaries. Therefore, idiosyncratic ICT risks at one entry point can become systemic, especially because they can trigger liquidity runs and an overall loss of confidence and trust in financial markets.

Figure 4. How cyber incidents could affect financial stability

[25] Boston Consulting Group, *Reigniting Radical Growth* (Global Wealth 2019), page 22.
[26] European Parliament report on *Fintech: the influence of technology on the future of the financial sector* (2016/2243(INI)).
[27] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.
[28] ESRB report *Systemic Cyber Risk*.



Source: Office of Financial Research, 2017 Financial Stability Report. U.S. Department of the Treasury[29]



Source: IMF, Cyber Risk Surveillance: A Case Study of Singapore, 2020[30]

A global consensus among authorities has formed that ICT risks are a source of *systemic* risk in the financial sector. Recent studies and papers published in Europe[31] and in the U.S.[32] demonstrate that ICT risk can threaten the stability of the entire financial system and that this type of risk can itself trigger a liquidity crisis and be a source of systemic risk (for more details on hypothetical scenarios see Annex 6). According to the IMF,[33] cyber events can propagate risks through the entire financial system and cause systemic risks via three broad transmission channels: risk concentration, risk contagion, and erosion of confidence. Although these channels are similar to the mechanisms of traditional financial shocks, a key difference lies in the speed by which risks materialise. Especially when driven by malicious intent (cyber-attacks), ICT risks can spread more quickly and at a larger scale, across sectors and beyond geographical borders, triggering liquidity runs and an overall loss of confidence and trust in financial markets. Critical functions that the financial sector provides to support the real economy (in particular deposit-taking and savings, lending, capital markets and investments, payments, clearing) may be impaired and may reverberate across other sectors of economy, in particular where the financial system itself faces difficulties in absorbing losses emerging from cyber-attacks and other large scale operational disruptions.

[29] https://www.financialresearch.gov/financial-stability-reports/2017-financial-stability-report/
[30] https://www.imf.org/~/media/Files/Publications/WP/2020/English/wpiea2020028-print-pdf.ashx.
[31] ESRB report *Systemic Cyber Risk* demonstrates that an operational disruption can lead to a systemic failure. The ESRB developed a conceptual model computing several amplifying factors that, if aligned, propagate the shock of a cyber-attack to provoke a systemic event.
[32] The Federal Reserve Bank of New York Staff Report on *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis* from January 2020 estimates that the impairment of any of the five most active US banks payment network could affect 38% of the US payment network. Additionally, if banks respond to uncertainty by refusing to lend (liquidity hoarding), the potential impact could reach more than 2.5 times daily GDP. Another paper focusing on the systemic nature of risk is the International Monetary Fund's *Cyber Risks Surveillance: A Case Study of Singapore*, February 2020.
[33] https://www.imf.org/~/media/Files/Publications/WP/2020/English/wpiea2020028-print-pdf.ashx.

2. PROBLEM DEFINITION AND SUBSIDIARITY

2.1. Problem definition

To be able to achieve digital operational resilience and adapt rapidly to changing business conditions, financial institutions should strengthen their ICT risk management (by developing a set of strategies and capabilities around governance, identifying and protecting against threats, responding and recovering from ICT-related disruptions, adopting an ICT change management policy, implementing an adaptive approach to incorporate into the framework lessons learned from past events, etc.), periodically test the effectiveness of their preventive and responsive capabilities integrated in the ICT risk management framework, share information with other financial institutions on actionable threat intelligence at strategical, tactical and operational level, report any major incident to financial supervisors, and manage risks stemming from their dependency on ICT third parties.

All these measures to address ICT risk are already implemented to a greater or smaller extent, and on a mandatory or voluntary basis. For instance, financial institutions are currently investing in ICT systems to strengthen their cyber security. However, these investments are unevenly distributed, and estimates show that about 10% of financial institutions make only very limited investments[34]. Furthermore, these investments currently take place in an environment where rules on digital operational resilience are not harmonised, and where accordingly supervisory expectations and requirements differ. This makes it more difficult for a firm to roll out effective, consistent and coherent responses aimed at addressing ICT risk across the group as a whole.

2.1.1. Fragmentation in managing ICT risks

Financial institutions in the EU operate within a set of legal requirements governing ICT risk alongside soft law measures, notably guidance and supervisory expectations enshrined at EU and/or national levels.

Drivers: The legal framework covering ICT risk and operational resilience across the financial sector is fragmented and not fully consistent. The regulatory provisions were developed at different moments in time, and seek to address the main risks identified at the time, hence they vary significantly across financial services sectors (see Annex 2). Some sectors (such as the Payment Services Directive – PSD2 or the Central Securities Depositories Regulation – CSDR) have specific and granular provisions for digital operational resilience. However, in other sectors (such as the Capital Requirements Directive – CRD IV, Solvency II for Insurance and Reinsurance, Credit Rating Agencies Regulation, Institutions for Occupational Retirement Directive – IORPS), the rules on ICT risk are scarce or limited only to high-level generic provisions. National requirements and supervisory guidance may fill some of these gaps, but not all and not necessarily in a consistent manner. ICT risk is addressed through operational risk requirements in EU financial services legislation, which are often and traditionally mainly quantitative (i.e. setting a capital requirement to cover the risk) rather than providing qualitative requirements aimed at protection, detection, containment, recovery and repair capabilities from operational incidents and failure.

[34] https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html.

In addition to the financial services legislation, a general framework covering a number of sectors and service providers governs the security of network and information systems under the NIS Directive. This is a cross-sectoral directive covering a number of economic activities deemed critical (see Annex 2), and that are rather diverse in their nature and market/cross-border integration. NIS being a minimum harmonisation directive, it has led to diversity in national transposition Its design revolves around the identification at national level of operators of essential services (OESs) and setting rules on "state of the art" security[35] and incident notification. For financial services, the NIS Directive covers OES in three areas of the financial sector, namely credit institutions, trading venues and central counterparties (CCPs). Under a *lex specialis* clause, EU sector-specific rules take precedence over NIS requirements when they are at least equivalent in effect to the NIS requirements. However, difficulties have arisen in this interplay, as well as divergences in implementing the NIS Directive to the financial sector. In its 2017 Communication,[36] the Commission specified that PSD2 is *lex specialis* for both security requirements and incident notification and that the Markets in financial instruments directive (MiFID) and the European Market Infrastructure Regulation (EMIR) are *lex specialis* for security requirements, which means they take precedence over the requirements of the NIS Directive. At the same time, Member States could add and some have added in their transposition additional sectors and national requirements at their own discretion.[37] It needs to be clarified that Directive 2008/114/EC on the protection of critical infrastructures (CIP), according to which Member States need to identify and designate European critical infrastructures and ensure risk assessments and reporting of incidents, does not cover the financial sector.[38]

Problem: Both the lack of specific ICT risk requirements in some subsectors and differences between such ICT risk requirements across financial subsectors and Member States leads to inconsistencies in protection, detection, containment, response and recovery capabilities for ICT related incidents between sectors and Member States. This leaves parts of the financial sector exposed to ICT related incident risks, without frameworks in place to address and manage these risks and makes the playing field uneven across the single market, with operators in some Member States being subject to specific requirements, whereas their competitors in other Member States are not subject to the same requirements. Further fragmentation and thus difficulties in compliance emerge for those financial institutions that operate on different financial sub-markets and have thus obtained several authorisations.

Consequences: The current disparity in rules puts at risk the financial sector's stability and integrity, as despite the interconnectedness of all parts of the financial sector, risks are

[35] According to Article 14(1) of the NIS Directive, Member States ensure that operators 'take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed'.

[36] Communication from the Commission to the European Parliament and the Council, *Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, COM/2017/0476 final.

[37] Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, COM/2019/546 final. Please also check Box 1 in section 2.2 for the difference between the basic concepts used in this impact assessment and the NIS definitions.

[38] On interdependencies between critical infrastructures in different sectors and the possible need to extend the scope of the Directive, please see the European Commission's evaluation of Directive 2008/114 on Critical Infrastructure Protection of 23 July 2019 (SWD(2019)308 final).

addressed and managed inconsistently across subsectors. As pointed out by the ESRB,[39] due to the highly interconnected nature of the financial system, the uneven level of ICT risk management can quickly cause problems in other segments of the financial sector. Furthermore, the current disparity of rules segments the single market for financial services, subjecting competitors to different requirements both in terms of scope and intensity.

The responses to the public consultation have shown extensive support to strengthen the ICT risk management framework for all financial institutions. Most respondents insisted that common standards should be principle and risk based and allow for proportionate application. They should ensure coherence in areas where currently, given the lack of more EU harmonisation, many financial institutions have voluntarily established and implemented security measures to manage and mitigate ICT risks, following national rules, EU soft rules (e.g. EBA guidelines) or global standards (e.g. International Organization for Standardization ISO).

2.1.2. Ineffective reporting of and limited awareness about threats and incidents

Under regulatory and/or supervisory requirements, financial institutions are subject to a number of ICT and operational *incident reporting* requirements to different authorities (see *type 1* in table 1 below). What use authorities can make of the incident notification information they receive, and whether and how they will share it with other authorities or market participants, depends on the regulatory and supervisory requirements under which the information is notified and the mandates of the respective authorities. Given the cross-border dimension of ICT risks and incidents, co-operation among competent authorities, including law enforcement where applicable, and *exchanging relevant information* (see *type 2* in table 1 below) in the incident reports they receive is necessary to effectively manage incidents or their consequences. Lastly, *information sharing among financial institutions* (see *type 3* in table 1 below) on threats and vulnerabilities contributes to increase awareness of ICT security and operational threats and to enhance the capacity to prevent threats from materialising into breaches or incidents, contain their effects or recover from them more efficiently.

The table below summarises the three main types of communication presented above:

Table 1 - Main types of communication on ICT-related incidents and threats

Incident reporting (type 1)	financial institution → competent authority
Exchange of information and cooperation (type 2)	competent authority → competent authority (also cross-border)
Information sharing (type 3)	financial institution → financial institution (possible collaboration with competent authorities)

Lack of incident reporting requirements in some financial subsectors

Few pieces of financial services legislation contain specific provisions on ICT incident reporting to authorities at either national or European level; most are silent on this. In the area of payments, PSD2 offers the most complete framework mandating the immediate reporting of an incident to the competent authority. It also enables - through EBA guidelines -

[39] The high level of interconnectedness across financial institutions, financial markets and financial market infrastructures, and particularly the interdependencies of their IT systems, constitute a potential vulnerability as a localised cyber incident could quickly spread across markets and jurisdictions. ESRB report *Systemic Cyber Risk*.

a classification and evaluation of reports, which creates a taxonomy that is useful in making incidents comparable. Investment firms engaged in algorithmic trading report material breaches in their electronic security measures,[40] and trading venues report incidents of misuse or unauthorised access. Data reporting service providers also report to competent authorities and notify clients affected by the breach. However, the financial services legislation covering most other areas (for example governing credit institutions, insurance undertakings or central securities depositories) does not establish reporting requirements. At the same time, the NIS Directive requires some of these institutions (certain credit institutions, CCPs and trading venues identified as OES, but not insurance undertakings, central securities depositories or asset managers) to notify incidents to the national NIS authority. Whether there is a single national NIS authority or whether sectoral authorities such as financial supervisors act as NIS authority in a Member State depends on national transposition and application of the NIS Directive.[41] Incidents amounting to breaches of the General Data Protection Regulation (GDPR) must be notified to data protection authorities.

Drivers: Since most pieces of EU financial services legislation remain silent or contain general wording on reporting of ICT-related incidents, some areas completely lack reporting to financial supervisors or NIS authorities. To fill these gaps, in some areas some financial supervisors have set up their own reporting schemes. For example, the SSM implemented its own set of requirements for its supervised banks, which comes on top of national financial services requirements, requirements under PSD2, application of the NIS Directive or the GDPR.

Problems: The lack of consistent information on the nature and consequences of ICT-related incidents impedes the proper calibration and implementation of prudential requirements and the development of suitable policy responses. At the same time, it means supervisors have an incomplete overview of the nature, frequency, significance and impact of incidents. Moreover, with no incident reporting in place, cybercriminal incidents remain unreported, information cannot be exchanged from financial supervisors to law enforcement authorities, and that ultimately impedes the investigation and prosecution of perpetrators and overall diminishes the deterrence of cybercrime.

Consequences: Notwithstanding ad hoc supervisory initiatives, the lack of consistent information on significant ICT related incidents in the financial system as a whole reduces public authorities' capability to assess and monitor risks that may affect the stability of the financial system, and to impose on financial institutions the necessary measures to prevent ICT-related incidents or limit their impact. There have been cases where financial supervisors were not made aware in time of cyber risks affecting other sectors. This undermines effective supervision and, ultimately, the objective of maintaining financial stability and market integrity.

Overlapping incident reporting

[40] According to Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment firms engaged in algorithmic trading, investment firms have to promptly inform the competent authority of any material breaches of their physical and electronic security measures and provide an incident report to the competent authority, indicating the nature of the incident, the measures taken following the incident and the initiatives taken to avoid similar incidents from recurring.

[41] According to Commission's data, around half of the Member States have designated their financial supervisors as the NIS authority for the financial sector, and other sectoral authorities for the other NIS sectors. The remaining half of the Member States have centralised it in a single national cybersecurity authority.

Drivers: Divergent transposition and implementation occurs mostly when dealing with minimum harmonisation directives, which are gold-plated by additional –more stringent- national rules. In addition, different frameworks give rise to multiple reporting obligations for the same ICT-related incident by a single financial institution. This may be necessary due to different angles under which the impact of an ICT breach can be analysed (e.g. an incident may impact personal data and, as such, it is brought to the attention of the data protection authorities for purposes other than the financial risk angle of financial supervision). This translates into financial institutions in fact having to report the same or different information on the same incident, under different legislation and to different authorities. For instance, as also revealed in the public consultation, a bank may have to report the same incident under the NIS Directive (if it has been identified as an OES and if the incident has a significant impact on the continuity of the bank's services), the SSM incident reporting framework (if it is a significant bank), under PSD2 (if the incident involves the payments side), under GDPR (if it affected the personal data of its customers) and under any other applicable national legislation.

Problem: Some financial institutions face complex, overlapping and potentially inconsistent reporting requirements for the same incident. The problem is amplified by differences in the taxonomy of ICT/operational incidents, reporting timeframes,[42] data sets, templates or applicable thresholds (triggering the reporting of an incident), as well as in the general approaches to consumer notification. Finally, the fragmentation becomes even more challenging for cross-border financial institutions that operate outside the EU and have to comply with additional requirements stemming from regulations from third country jurisdictions. Responding companies to the public consultation are currently subject to multiple ICT and security incident reporting requirements that either stem from regulation (e.g. GDPR, eIDAS, national rules transposing PSD2, NIS, or other national laws), supervisory expectations (e.g. SSM, TARGET2) or industry best practices. A concrete example would be the case of a big bank that has been identified under the NIS transposition as operator of essential services in one Member State and is also licenced as payment service provider under PSD2. In this case, incident reporting obligations deriving from the legislation overlap if the *lex specialis* clause is not upheld in that Member State; to this overlap, one has to add the incident notification under the SSM framework for significant banks. The bank should not report major incidents to the NIS authority in that Member State because it also operates under PSD2 (and the *lex specialis* is supposed to do away with the overlap). However, because the NIS transposition has been quite fragmented, it must report the same incident to the financial supervisor, to the NIS authority and to the SSM, under different criteria and patterns. A big subsidiary of this bank in another Member State, for example, even if providing services deemed essential under the national transposition of the NIS Directive, would not have to report to the NIS authority because the transposition of the NIS Directive took the *lex specialis* into account.

Consequences: Having to report the same incident to multiple authorities leads to excessive administrative burden and compliance costs at times when financial institutions must also focus resources on managing and containing the incident and recovering from it. Respondents to the public consultations stressed that the myriad of different requirements creates a significant compliance burden for them without a corresponding improvement in security. In addition, all these different criteria lead to fragmentation in the overall incident reporting requirements, possibly amplified by any different interpretations across legislations, with

[42] For instance, whereas reporting an incident under the NIS Directive should be done without "undue delay", the deadline is 72 hours under GDPR, 4 hours under PSD2 and 48 hours under Target2.

authorities having only partial insights into how ICT and operational incidents affect the financial sector.

Absence at EU level of trusted mechanisms enabling cyber threat intelligence sharing between financial institutions

Drivers: With cyber, ICT and operational threat landscapes becoming complex and sophisticated, good detection and prevention measures depend to a great extent on regular threat and vulnerability intelligence sharing between financial institutions. However, a number of factors inhibit intelligence and information sharing in relation to threats, in particular a lack of trust and of suitable mechanisms and arrangements. Financial institutions also express doubts or concerns about whether information sharing is legally possible and commercially feasible between peers. In particular, respondents to the public consultation cited concerns over compatibility with data protection and anti-trust requirements, or even liability (for more details see point 3.2 of Annex 3). Hesitations about what can be shared – other than incidents- with other market participants, with competent authorities, e.g. financial supervisors in their oversight function, the European Union Agency for Cybersecurity (ENISA) for analytical input or Europol for law enforcement purposes, leads to information being withheld.

Problem: As the ICT risk dimension has only gradually and partially been addressed across the EU financial services legislation, the extent of information sharing among financial institutions in relation to threats, as well as the quality of such information (when shared) is limited, fragmented and mostly local (national initiatives), with no consistent EU-wide information sharing arrangements tailored for the real needs of the financial sector and authorities. Since financial institutions cannot leverage in a collective manner their individual knowledge and practical experience, their understanding of the cyber threats also remains fragmented and isolated. This prevents threat-informed decisions to help build up defensive capabilities, threat detection techniques and mitigation strategies. The lack of correlation between different types of cyber information and intelligence from multiple sources, for instance indicators of compromise such as system artefacts or observables associated with an attack, motives of threat perpetrators, and security alerts, which weakens financial institutions' efforts to successfully withstand malicious attacks.

Consequences: Insufficient information sharing and cooperation on cyber threat intelligence at strategical, tactical and operational level (on, for example, indicators of compromise or techniques used by cyber criminals) ultimately prevent individual financial institutions from adequately assessing, monitoring, defending against and responding to cyber threats. Moreover, the lack of information sharing in trusted environments undermines the ability of the financial community to prevent and respond collectively by quickly limiting the spread of cyber risks and operational threats and impeding potential contagion throughout financial channels.

2.1.3. Limited and uncoordinated testing

To achieve robust digital operational resilience, in line with international standards (e.g. the G7 Fundamental Elements for Threat-Led Penetration Testing (TLPT))[43], institutions should

[43] The G-7 Fundamental Elements for Threat-Led Penetration Testing (G7FE-TLPT) provide entities with a guide for the assessment of their resilience against malicious cyber incidents through simulation and a guide for authorities considering the use of Threat-Led Penetration Testing (TLPT) within their jurisdictions. The core objectives of the

regularly test their ICT systems and governance as to the effectiveness of their preventive, detection, response and recovery capabilities, to uncover and address potential vulnerabilities. Responding to differences across and within financial sectors regarding the maturity level of financial institutions' cybersecurity preparedness, testing should include a wide variety of tools and actions, ranging from simple assessment of basic requirements (e.g. gap analyses, compliance reviews, vulnerability scans) to more advanced testing (e.g. TLPT for significant financial institutions capable of carrying out such tests)[44]. The majority of respondents to the public consultation agree that financial entities should be required to perform a baseline testing/assessment of their ICT systems and tools.

Drivers: Regarding the current testing exercises carried out in the EU, the problem is twofold: (1) in some financial subsectors, there are multiple and uncoordinated penetration and resilience testing frameworks and requirements that address the same issues in a different way, with the subsequent duplication of costs for the tested financial institutions and no cross-border recognition of results and (2) other subsectors lack penetration and resilience testing frameworks.

To map the resilience testing practices in the EU, the EBA conducted a survey on supervisory practices on cybersecurity, which identified many differences in testing requirements, the process of testing, cross border cooperation on such testing and sharing of the testing results. The survey revealed that only a few authorities organised penetration testing or gave guidance on such testing. Most respondents indicated not having pen-tested financial institutions' vulnerability and resilience to cyber risks.

In 2018, the ECB published a framework for threat intelligence-based ethical red teaming (TIBER–EU). This is a common framework that delivers a controlled, bespoke, intelligence-led red team test of financial institutions' critical live production systems. TIBER-EU is designed to be adopted by competent authorities in any jurisdiction, on a voluntary basis and for a variety of prospective uses, in particular as a supervisory or oversight tool, for financial stability purposes, or as a catalyst in collaboration with market participants.

Although a number of Member States and supervisors have developed and/or are in the process of implementing digital operational resilience testing frameworks, some inspired by TIBER-EU, the frameworks present certain similarities, but also differences in terms of scope, testing methods and the requirements or authorities involved.

Problems: Without the establishment of at least a common set of rules in guiding these tests, the frameworks are not applied coherently. Moreover, there is no mutual acceptance of the testing results between Member States, and financial institutions active in multiple jurisdictions are subject to multiple testing frameworks and requirements on the same ICT infrastructure. Respondents to the public consultation face issues with overlapping or diverging testing obligations for ICT and security tests by different authorities, which tie up considerable resources. In many financial subsectors there is also no knowledge exchange at

---

G7FE-TLPTare to enhance and assess the cyber resilience of entities and the financial sector more generally. See: https://www.bundesbank.de/resource/blob/764690/792725ab3e779617a2fe28a03c303940/mL/2018-10-24-g-7-fundamental-elements-for-threat-led-penetration-testing-data.pdf. TLPT is a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat perpetrators. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal fore-knowledge and impact on operations. In some jurisdictions this may be referred as Ethical Red Teaming.

[44] The different testing tools should not be sector specific, but instead differ across and within financial subsectors depending on financial institutions' level of cyber security preparedness.

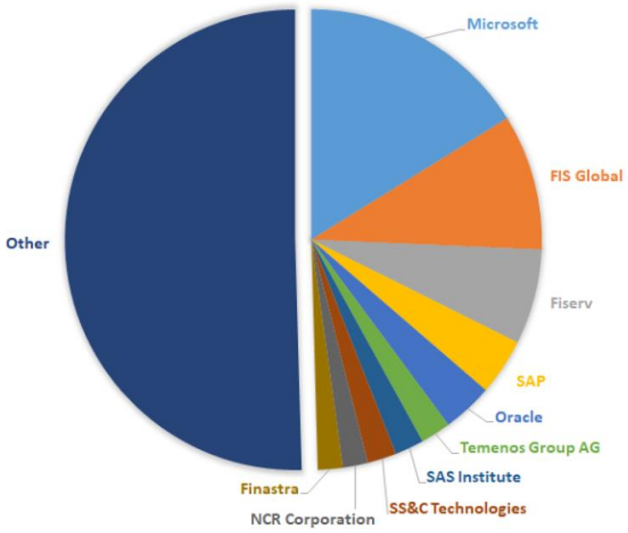
EU level between competent authorities, which means best practices are not shared between financial institutions or between them and competent authorities. In addition, where there is no testing, vulnerabilities remain undetected and can and will be exploited by threat perpetrators.

Consequences: Uncoordinated testing can potentially segment the single market and undermine the single or coordinated supervisory approach. At the same time, the lack of cross-border acceptance of test results among supervisory authorities generates additional burden and costs for financial institutions. This makes the level playing field uneven, as evidenced by the responses to the public consultation (for more details see point 3.3 of Annex 3). When there is no testing and vulnerabilities hence remain undetected, the financial sector stability and integrity is at higher risk.

2.1.4. ICT third-party risks

Financial institutions have increased the use of third-party providers (TPPs), in particularly for the provision of ICT products and services. Financial institutions enter into contractual relationships with ICT TPPs whereby they outsource the performance of some of their operational functions. In particular, the use of cloud services has recently been the focus of much attention. According to the FSB,[45] the deployment of cloud technologies in the financial service industry is still in an early phase, with around 70% of financial services companies reporting in a recent survey that they were only at the initial or trial and testing stage. However, the use of cloud services is patchy across different financial operators and financial subsectors, and there is high potential for growth. Markets and Markets[46] predicts that the financial cloud market will grow at a rate of 24% to reach more than $29 billion by 2021. A recent Bloomberg survey of Europe's top banks revealed that 22 of 22 respondents use Amazon, Microsoft, or Google[47]. According to the Institute of International Finance (IIF), Amazon Web Services have almost 50% of market share, followed by Microsoft Azzure, Google, IBM or Alibaba.

Figure 5. Market share of ICT vendors in financial service industry, 2018



[45] https://www.fsb.org/wp-content/uploads/P091219-2.pdf.
[46] https://www.marketsandmarkets.com/Market-Reports/finance-cloud-market-1053.html.
[47] https://www.bloomberg.com/news/articles/2020-03-06/european-banks-store-their-sensitive-data-on-american-clouds.

Source: Apps Run The World[48]

The dependence on ICT third parties was also highlighted in the ESAs joint technical advice, which suggested an appropriate oversight framework be applicable to the activities of ICT TPPs that are *critical* service providers to financial institutions.[49] The extent and nature of this reliance has amplified in recent years, driven by an effort from financial institutions to adapt to the digital economy, boost efficiency and remain competitive, as well as meet consumer demand.

The main incentives to rely on third parties for the provision of ICT products or services are performance, reliance, elasticity of ICT resource provisioning and cost-effectiveness. The aim of financial institutions when accessing innovative technologies offered 'as a service', for instance cloud adoption, may be to source alternatives for outdated, on-site legacy ICT infrastructure, which can be very costly to maintain and upgrade, and less flexible in accommodating the institution's ICT needs to embrace innovation and ensure security. The use of ICT TPPs by financial institutions is not limited to cloud service providers. Most financial institutions also use specialised ICT TPPs for products and services that they cannot develop in-house (e.g. specialised software, hardware, etc.), or where such in-house features would fall below the standards that TPPs are able to provide.

The operations of ICT TPPs entail significant risks for financial institutions (for example in handling financial data). Almost 60% of surveyed companies experienced a data breach caused by a third party, according to the Ponemon Institute.[50] Such risks are predominantly micro-prudential and, if at all addressed by the existing regulatory framework, addressed to varying degrees: governance risks, operational risks (security and privacy, integration, portability, and interoperability between systems), vendor lock-in,[51] confidential data risks, fourth party and supply chain risks (given the increasing tendency of some TPPs to sub-contract parts of the services they provide to additional vendors), legal and compliance risk (e.g. when operational incidents or poor performance at a TPP prevent a financial institution from complying with its regulatory reporting obligations), reputational risks and lack of explainability.[52]

Moreover, the widespread use of a limited number of closely connected ICT TPPs by a large number of financial institutions can lead to macro-prudential risks, such as concentration and systemic risks. This can adversely impact financial stability in the event that one or more of the critical providers experience a major disruption in providing their services. That conclusion stands irrespective of the root cause (e.g. be it a malfunction or a major cyber-attack).

[48] https://www.appsruntheworld.com/top-10-banking-and-financial-services-software-vendors-and-market-forecast/

[49] ICT TPPs in this respect include, for example, data providers and cloud services providers. The designation of critical TPPs would be based on both quantitative and qualitative criteria (e.g. number and systemic significance of institution customers (size) with domestic/regional/global impact, interconnectedness, substitutability, multi-jurisdictional activity, complexity, etc.).

[50] 2018 Data Risk in the Third Party Ecosystem Study from Ponemon Institute https://www.ponemon.org/local/upload/file/Data%20Risk%20in%20the%20Third%20Party%20Ecosystem_BuckleySandler%20LLP%20and%20Treliant%20Risk%20Advisors%20LLC%20Ponemon%20Research%202016%20-%20FINAL2.pdf.

[51] Vendor lock-in happens when financial institutions are dependent on a single TPP for a relevant service and cannot switch to another TPP without substantial costs, substantial inconvenience or in an appropriate period of time. It can amplify when only one or a small number of third parties dominate the provision of a given service and/or if institutions do not mitigate their dependence on these third parties with an effective documented and tested exit strategy.

[52] Lack of explainability (also called 'black box') relates to the inability of financial institutions to understand or explain actions, decisions or recommendations made or facilitated by TPPs, such as Artificial Intelligence/Machine Learning.

Limitations and difficulties for financial institutions to ensure compliance with the regulatory framework on outsourcing and further sub-outsourcing arrangements

Drivers: As financial institutions become more and more dependent on products and services provided by ICT TPPs, they also face higher levels of risk exposure, both of a micro and macro prudential nature, towards providers outside the financial sector, who are unregulated and thus unmonitored by financial supervisors. The burden for ensuring TPPs' compliance with the regulatory framework remains on the financial institutions. Without prejudice to their contractual freedom, the regulatory framework requires financial institutions to remain fully responsible for their outsourcing arrangements; some must draw them in writing and notify financial supervisors of their outsourcing arrangements and sometimes get the supervisors' approval (please see section 4 of Annex 2). That is because outsourcing entails critical or important operations or functions that financial institutions should in principle deploy in house and because such business arrangements impact financial institutions' compliance with their prudential regulatory obligation to monitor and address operational risks.

One of the most complicated problems that financial institutions and supervisors acknowledge today is their lack of ability or actual power to monitor risks in the sub-outsourcing value chain. In addition, financial institutions often have difficulties in negotiating written agreements tailored to their prudential legal and regulatory requirements or cannot fully enforce rights of access as stipulated in contracts with ICT TPPs. Their initial contract with the TPP often does not provide for sufficient safeguards on how the sub-outsourcing process should be monitored (i.e. no notification of the sub-outsourced services, lack of relevant information on the type of function further sub-outsourced or on the actual location or jurisdiction where the sub-outsourcing is performed). This may be the result of a high degree of asymmetry in negotiating positions between financial institutions and hyper-scale technology providers, which leads to contractual limitations or gaps (e.g. on rights to access, audit and obtain information from TPPs).

The public consultation highlighted a large number of additional challenges during contractual negotiations between financial institutions and ICT TPPs, such as the geographical storage of data, sub-contractor approval and transparency, information rights, exit strategies, post-termination assistance, resolution requirements, business continuity clauses, etc. (see section 3.4 on page 10 of Annex 3). At the same time, supervisors are not getting the insights they need into the solutions and risks presented by ICT TPPs. According to the Ponemon Institute, companies are not able to (i) confirm whether third parties have had a data breach or cyber-attack involving their sensitive and confidential information, (ii) determine the number of third parties with access to their confidential information, and (iii) verify whether the third party can sufficiently respond to a data breach or cyber-attack.

Problem: When the contractual relationship entails outsourcing and sub-outsourcing of core functions or operations of a financial institution, this lack of control may impair the continuity and security of the performance of the financial services that are outsourced. Currently, the *indirect supervision* performed by financial supervisors over the supervised financial institutions, who in turn ought to have robust contractual terms and conditions in their outsourcing arrangements guaranteeing the performance (or in its absence, the liability) of the outsourced activities or functions by TTPs does not address concentration and systemic risks posed by ICT TPPs to the financial system.

Consequences: The inability to enshrine contractual rights tailored to the prudential requirements for outsourcing that financial institutions must abide to, the difficulty to enforce

these rights, and the lack of supervisory insights into the activities of financial institutions which are provided by ICT TTPs (with all risks associated) expose financial institutions individually, and the financial system as a whole, to operational risks which, even though they originate at a third party (or further along the sub-outsourcing chain), have direct consequences on the actual performance of financial institutions, and hence on the stability and integrity of the financial service or system. These risks remain outside the purview and perimeter of proper, direct and consistent EU financial services regulation and supervision.

Unmonitored ICT third-party providers

Drivers: Currently, there is no EU-wide[53] direct oversight framework to enable financial supervisors to effectively monitor the activities of critical ICT TPPs in relation to the services they provide to financial operators.[54] Some steps were taken under the EBA guidelines on outsourcing to require banks, investment firms, payment and e-money institutions to maintain and update a register of all outsourcing arrangements with cloud service providers. Financial institutions and cloud service providers joined forces to develop a template for the register, but the register will be available only as of December 2021 and it has some limitations (e.g. it covers only outsourcing arrangements with a subset of ICT TPPs - cloud service providers, it has a limited coverage of the supply chain, no common templates for data reporting). Most importantly, the register applies only to the financial entities mentioned above and there is no comparable inventory or register applicable to other financial institutions. This could also result in asymmetries in the volume of information available to supervisory authorities.

According to the results of the public consultation, a typical European financial institution accesses over 1,000 different cloud services, many unapproved and unlikely to be monitored. Employees and partner organisations may use ICT systems that are not monitored, managed or secured. These third parties could greatly increase operational risks and yet the competent authorities' oversight over some ICT (cloud) TPPs is inadequate. Furthermore, some respondents complain that relevant ICT TPPs are not regulated within the EU.

The above-mentioned increased reliance of financial institutions on ICT TPPs is only partially addressed in EU legislation via requirements imposed on financial institutions to notify their outsourcing arrangements to supervisors and the general principle that financial institutions retain full responsibility for their contractual relationships. Higher risk exposure and the concentration and systemic risks originated at the unregulated entity offering the outsourced service or platform are not explicitly captured by the current legal framework. This translates

[53] To be noted that in other parts of the world, some jurisdictions do have arrangements for financial supervisors to oversee/supervise third party providers. For instance, in the US, the Bank Service Company Act governs permissible bank service company activities, regulatory approval of bank investments in service companies, and regulation and examination of bank service companies. The Board of Governors of the Federal Reserve System (FRS), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (each individually, Agency, and collectively, Agencies) have statutory authority to supervise third-party service providers entering into contracts with their regulated financial institutions. The "Supervision of Technology Service Providers" booklet (TSP Booklet), of the FFIEC Information Technology Examination Handbook (IT Handbook), addresses and outlines the Agencies' risk-based supervisory program, and while technology service providers (TSP) examinations generally focus on underlying information technology (IT) risk, the risk assessment also considers all business lines in which TSPs engage to ensure that all covered services are effectively included. The Agencies conduct IT-related examinations of financial institutions and their TSPs based on the guidelines contained in the FFIEC IT Handbook. Source: EBA discussion note on TPPs oversight framework, SCOP 2020 30, March 2020.

[54] According to NIS, cloud service providers (as one category of digital service providers falling under the NIS Directive) are subject to ex post supervision carried out by the designated NIS authority. The supervision is limited to the security and notification requirements imposed on them by the NIS Directive.

in practice into different supervisory approaches that are based on the supervisors' general mandate to monitor operational risks:

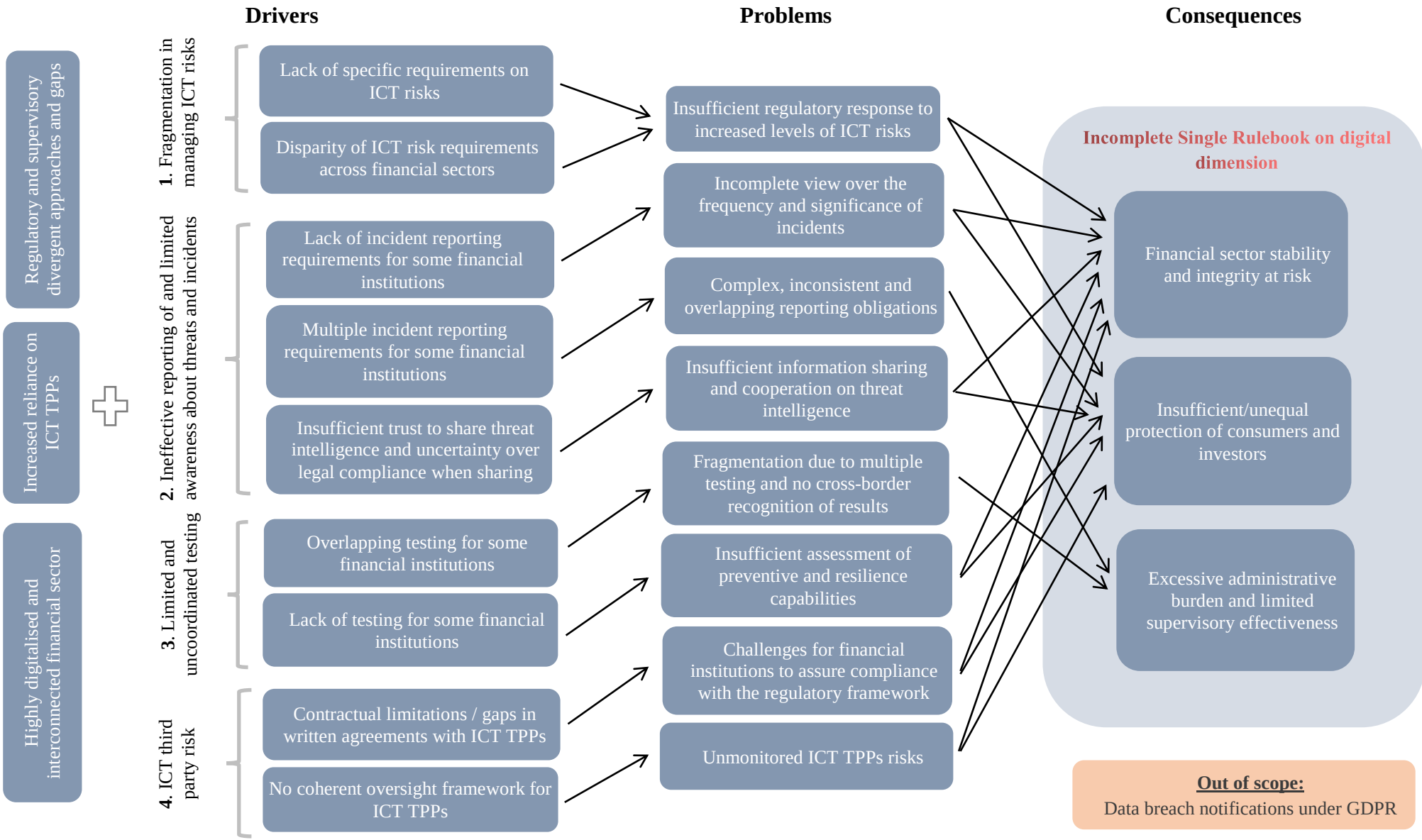
(1) some supervisory authorities are hesitant to allow financial institutions to enter into contractual arrangements with ICT TPPs, as supervisors either have insufficient insight into whether ICT third parties present risks or do not always possess all the tools they need to analyse and oversee the impact of these third-party dependencies;

(2) other supervisory authorities, although they allow such contractual arrangements, still require financial institutions to obtain approval before outsourcing to ICT TPPs and impose diverging requirements on financial institutions.

Problem: In the absence of EU or national rules tackling risk exposures to critical entities outside the financial sector, that have the potential to jeopardize overall financial stability, either risks remain unaddressed or diverging and unsatisfactory administrative practices emerge. Supervisors are not equipped with a sufficient mandate, nor the tools and expertise to monitor and manage concentration and systemic risks stemming from financial institutions' outsourcing of important functions and subsequent third party dependencies.

Consequences: In a highly interdependent financial system, which is interlinked across the EU, concentration and systemic risks are not effectively contained or unilaterally addressed due to uncoordinated supervisory approaches at national level. In the absence of an EU coherent oversight framework, the Single Rulebook does not offer fully appropriate mechanisms and tools that supervisors need to be able to quantify, qualify, address and redress operational, concentration and exposure risks vis-a-vis critical ICT TPPs. The ensuing reluctance of supervisors to allow financial institutions to make greater use of ICT TPPs also hampers the adoption of potentially more cyber-resilient ICT solutions provided by ICT TPPs.

Problem tree



2.2. The EU's need to act and justification

2.2.1. Legal basis

The Treaty on the Functioning of the European Union confers to the European institutions the competence to lay down appropriate provisions for the approximation of laws of the Member States, that have as their objective the establishment and functioning of the internal market (Article 114 TFEU). This encompasses the power to enact legislation at EU level to approximate prudential, market conduct and other relevant requirements for financial institutions and for their supervisors. As financial services are currently overwhelmingly deployed through varied and complex ICT-based systems and processes, and likely to become even more so in future, there is a clear need that all financial operators understand and remain at all times in full control of the ICT risks deriving from their use of technological solutions, including their third party dependencies. This initiative aims to remove obstacles to and improve the establishment and functioning of the internal market for financial services by ensuring the applicable rules are fully harmonised. The current disparities in the area of ICT risk management, testing and third party risk, both at legislative and supervisory level, and both at EU and national level, act as obstacles to the single market in financial services: financial institutions with cross-border activities face different and at times overlapping regulatory requirements or expectations, that have the potential to impede their exercise of freedom of establishment and provision of services; competition between the same type of financial institutions in different Member States is also distorted. Moreover, in areas where EU harmonisation is absent or partial/limited (e.g. digital operational testing framework, oversight of activities of critical ICT TPPs), the divergent development of national rules or approaches, which have either been adopted or are in the process of adoption and implementation at national level, could also act as deterrents to the single market freedoms for financial services.

2.2.2. Subsidiarity: Need for EU action

Digital operational resilience is an issue of common interest to the EU's financial markets. It is essential for the proper functioning of the EU financial sector, especially in the digital age. The level of integration within the EU financial sector - governed by EU regulation and supervision - together with the cross-border activity of financial institutions, and the depth and breadth of digitalisation set the financial sector apart from other sectors. Without completing the European Single Rulebook with operational provisions and tools to address ICT risks and incidents that it currently lacks, all other types of risks would be tackled at European level, but digital operational resilience would remain either left out or subjected to fragmented and uncoordinated national-level initiatives. The potentially significant levels of investment required also highlight that diverging requirements have very real impacts on the level playing field in the internal market. All this currently segments financial markets and could further make the playing field uneven.

The interdependencies so typical of the financial sector are such that individual financial institutions very often cannot fully handle the threats, manage the risks and the possible impacts of ICT incidents on their own. ICT threats and risks have a cross-border dimension that poses operational challenges. Those interdependencies across Member States make public intervention at EU level not only beneficial, but needed. The current disparities resulting from uneven frameworks applicable to different financial institutions and to different financial subsectors and also to the same financial institution operating cross-border and/or holding several authorisations (e.g. one financial institution can have a banking, an

investment firm, and a payment institution licence, every single one issued by a different supervisor in one or several Member States) across the Member States can thus only be tackled at EU level. The initiative would harmonise an area of the economy that is so deeply connected, integrated, interdependent and that already benefits from a single set of rules and supervision.

In terms of incident reporting, only harmonised EU-level action could reduce the reporting burden - and the implicit costs - of the same ICT-related incident being reported to different EU and/or national authorities. EU action is needed also to facilitate the mutual recognition/acceptance of the testing results of institutions operating cross-border that are subject to different testing frameworks in different Member States. Some Member States have put in place (or are considering) national testing frameworks, some based on TIBER-EU, and some diverging from it. Furthermore, although some risks are mitigated in the Members States that introduced specific testing obligations, in others those risks remain unaddressed and unmonitored and this distorts competition. Financial institutions also rely on service providers and infrastructures located across the EU; the lack of an appropriate and coherent oversight framework to monitor risks stemming from ICT TPPs, including concentration and contagion risks at EU level, also benefits from EU-wide action.

Finally, it should be noted that GDPR notifications are out of scope in this initiative since they are imposed by the GDPR which pursues a distinct objective, and cover only a sub-sector of cases (e.g. those where personal data is concerned).

2.2.3. Subsidiarity: Added value of EU action

In the current context and looking at future scenarios, it appears that, to increase collective digital operational resilience for the financial system as a whole, individual action by Member States and a fragmented approach is suboptimal and clearly insufficient. EU action is deemed necessary to address fragmentation in ICT risk management, the testing frameworks, overlapping incident notifications and the mechanisms and tools needed to contain ICT third party risk. Action at EU level would bring more advantages and greater value than action taken separately at national level. It would provide legal clarity on whether and how digital operational provisions apply, especially to cross-border financial institutions, and it would eliminate the need for Member States to individually improve rules, standards and expectations regarding operational resilience and cybersecurity as a response to the limited coverage of EU financial rules and the general nature of the NIS Directive. However, EU intervention would not impact on the NIS Directive, as it would build on it and address any possible overlaps via a *lex specialis* exemption. The interaction between financial services regulation and the NIS Directive would continue to be governed by a *lex specialis* clause, which would continue to exempt financial institutions from the substantive NIS requirements and avoid overlaps between the digital operational resilience act and the NIS review. In addition, the interaction with the European Critical Infrastructure (ECI) Directive[55] would be in a similar way as it today co-exists with the NIS Directive.

Not taking action at EU level would be a missed opportunity to reap the full benefits of the single market, as the proliferation of piecemeal and uncoordinated approaches at national level would continue. This is particularly the case, in light of the ongoing COVID-19 crisis,

[55] To be noted that the ECI Directive (Directive 2008/114/EC) does not cover the financial sector and was adopted under Article 352 TFEU, which does not entail harmonisation and requires unanimity, and has the objective to protect physical infrastructure. It has therefore a different objective than the present initiative focussed on digital operational resilience.

whereby different measures to support operational resilience were taken at national level.[56] The benefits of digital finance in continuing to serve customers remotely during the crisis illustrate even more acutely the need to ensure heightened and coordinated operational resilience. Because the COVID-19 crisis is likely to provide even further impetus to the digitalization of financial services, that should come hand in hand with further emphasis on ensuring a coordinated digital operational resilience. An EU-wide framework would significantly increase the effectiveness of the policy while also reducing complexity, and easing the financial and administrative burden on all operators. By way of example, the decision to incorporate the Basel standards into EU legislation over ten years ago has proven to be a success story: as a result, European banks are now much better capitalised and follow a single set of rules applicable throughout the EU thanks to a decision to act at EU and not at national level.

In accordance with the principle of **proportionality**, the proposed rules will not go beyond what is necessary in order to achieve the objectives set out in section 3 below. The initiative will cover only the aspects that Member States cannot achieve on their own and where the administrative burden and costs are commensurate with the specific and general objectives to be achieved. Proportionality will be carefully designed in terms of scope and intensity and using qualitative and quantitative assessment criteria to ensure that the new rules will cover all financial subsectors and institutions, but will be tailored to the specific risks they face and the needs they must address; as such, proportionality will be embedded to different degrees in the different rules on ICT risk management, basic and advanced testing, reporting of major incidents and oversight of critical ICT TPPs. None of the options analysed in this impact assessment goes beyond what is necessary to achieve the objectives set in the following section. EU action is therefore justified on both grounds of subsidiarity and of proportionality.

3. OBJECTIVES

In light of the problems outlined in the previous chapter, the overall objective of the initiative is to strengthen the **digital operational resilience** of the EU financial sector entities by streamlining and upgrading existing rules and bringing in new requirements where there are gaps. This would also enhance the Single Rulebook on its digital dimension. Moreover, the initiative would seek to maximise the benefits associated with the horizontal framework (e.g. NIS Directive), and as such contribute to the overall resiliency of the EU economy. The initiative will duly take into account recommendations endorsed at international level, as well as existing EU and national frameworks on ICT risk management and operational resilience.

The overall objective can be structured in three general objectives:[57]

[56] Annex 1 - Financial policy measures taken in response to COVID-19 pandemic (as of 11 April 2020) of the FSB *COVID-19 pandemic: Financial stability implications and policy measures taken* (15 April 2020) show in the last column the measures taken by some Member States to support operational resilience (Netherlands, Germany, Italy, France), which do not coincide with those taken at EU level.

[57] There is a growing consensus among Member States and private stakeholders on the need to reduce regulatory fragmentation and to address gaps within the current EU financial services regulatory framework. The Commission carried out a public consultation on digital operational resilience in the financial sector between December 2019 and March 2020, which revealed broad support for EU-wide harmonisation. Respondents called for all financial entities to (1) have in place an ICT risk management framework based on key common principles, (2) report major incidents using uniform criteria, templates and mechanisms and to a single authority, (3) regularly update, test and review ICT systems and tools in order to withstand cyber-attacks or ICT-related disruptions and to assure operational resilience. Respondents also expressed the need to manage third party risk via outsourcing rules and an EU oversight framework (for more details see Annex 3).

- **Reduce the risk of financial disruption and instability**: an EU digital operational resilience framework for the EU financial services would enhance the security and resilience of the financial institutions and market infrastructures and reduce the risks to financial stability. This would translate into the following specific objectives:
    - Address ICT risks more comprehensively and strengthen the overall level of digital resilience of the financial sector;
    - Enable financial supervisors' access to information on ICT-related incidents;
    - Ensure that financial institutions assess the effectiveness of their preventive and resilience measures and identify ICT vulnerabilities;
    - Strengthen the outsourcing rules governing the indirect oversight of ICT TPPs;
    - Enable a direct oversight of the activities of ICT TPPs;
    - Incentivise the exchange of threat intelligence in the financial sector.
- **Reduce the administrative burden and increase supervisory effectiveness**: the different overlapping incident reporting obligations should be streamlined and simplified to reduce the administrative burden for the financial institutions. In addition, a coherent EU digital operational resilience testing framework would contribute to reduce costs resulting from multiple testing, duplication of work and additional burden for financial institutions within the EU financial sector. This would translate into the following specific objectives:
    - Streamline ICT-related incident reporting and address overlapping requirements;
    - Reduce single market fragmentation and enable cross-border acceptance of testing results.
- **Increase consumer and investor protection:** the envisaged measures in the initiative would be addressed to financial institutions. However, strengthening the overall digital operational resilience of the EU financial sector would also (indirectly) contribute to increasing both consumer and investor protection.

Table 2 – Intervention logic diagram

Drivers of the problems	Identified problems and their consequences	Objectives
	<u>Consequence 1 of the identified problems</u> **Financial sector stability and integrity at risk**	**<u>General Objective 1</u>** **Reduce the risks to financial sector stability and integrity**
• Lack of specific requirements on ICT risks • Disparity of ICT risk requirements across financial sectors	• **Problem 1**: Non-specific and insufficient regulatory response to increased levels of ICT risks	• **Specific objective 1**: address ICT and security risks more comprehensively and strengthen the overall level of digital resilience of the financial sector
• Lack of incident reporting requirements for some financial institutions	• **Problem 2**: Incomplete view over the frequency and impact of ICT-related incidents	• **Specific objective 2**: enable financial supervisors' access to information on ICT-related incidents
• Lack of testing for some financial institutions	• **Problem 3**: Insufficient assessment of preventive and	• **Specific objective 3**: ensure that financial institutions assess the

	resilience capabilities	effectiveness of their preventive and resilience capabilities and identify ICT vulnerabilities
• Contractual limitations / gaps in written agreements with ICT TPPs	• **Problem 4:** Challenges for financial institutions to assure compliance with the regulatory framework when certain functions are outsourced or further sub-outsourced	• **Specific objective 4:** strengthen the outsourcing rules governing the indirect oversight of ICT TPPs
• No coherent oversight framework for ICT TPPs	• **Problem 5:** Unmonitored ICT TPPs risks that lead to financial stability concerns linked to concentration risk	• **Specific objective 5:** enable a direct oversight of the activities of ICT TPPs
• Insufficient trust to share threat intelligence and uncertainty over legal compliance when sharing	• **Problem 6**: Insufficient information sharing and cooperation on threat intelligence	• **Specific objective 6**: incentivise the exchange of threat intelligence in the financial sector
	Consequence 2 of the identified problems **Excessive administrative burden and limited supervisory effectiveness**	**General Objective 2** **Reduce the administrative burden and increase supervisory effectiveness**
• Multiple incident reporting requirements for some financial institutions	• **Problem 1**: Complex, inconsistent and overlapping reporting obligations	• **Specific objective 1**: streamline ICT-related incident reporting and address overlapping requirements
• Overlapping testing for some financial institutions	• **Problem 2**: Cost of compliance with multiple testing and lack of cross-border recognition of testing results	• **Specific objective 2**: reduce costs (and single market fragmentation) and enable cross-border acceptance of testing results
	Consequence 3 of the identified problems[58] **Insufficient/unequal protection of consumers and investors**	**General Objective 3** **Increase consumer and investor protection**

4. OPTIONS AND ASSESSMENT OF POLICY OPTIONS

This section will examine the policy options available and their estimated impacts in achieving the objectives presented in Table 2:

- **"Do nothing" scenario**: No change in the EU financial services regulatory framework;
- **Option 1**: Strengthening financial institutions' ability to absorb losses stemming from lack of digital operational resilience;
- **Option 2**: A financial services digital operational resilience act;
- **Option 3**: A financial services digital operational resilience act together with centralised supervision of activities of critical ICT TPPs.

[58] This is an additional (indirect) consequence from problems 1 to 6, as described in the description of the general objectives.

The below policy matrix summarises each of the options (in the rows) along with the related four policy areas to be addressed (in the columns) in light of the problems and objectives specified above. The four policy areas have been identified because they are the four key inter-related pillars included consensually in European and international guidance and best practices (e.g. ECB, G7, FSB, BCBS, etc.) aimed at enhancing the cyber and operational resilience of the financial sector. The four policy areas are therefore the "state of the art" which any EU initiative which aims at reducing the risks to financial sector stability and integrity from cyber and operational risk (general objective 1 and related sub-objectives) must address. These are also the areas that existing fragmented rules and supervisory activities at European and national level cover, and hence any initiative aimed at reducing the administrative burden and increase supervisory effectiveness (general objective 2 and related specific objectives) must cover them.

The digital operational resilience act aims to strengthen the digital operational resilience of the EU financial sector by addressing the different issues reflected in the "state of the art" of international and European work. Achieving this objective can be pursued in different ways (e.g. quantitative vs. qualitative approach) and with different levels of integration (e.g. supervisory cooperation vs. new authority to oversee ICT TPPs). This is reflected in the different options assessed in this section.

In the below matrix, each cell outlines the specific measures and level of ambition foreseen in each policy area. More specifically:

- The first column, *ICT risk management*, refers to the main elements of the risk management framework for building a proper digital operational resilience core requirements for the financial sector (e.g. requirements on governance, on ICT risks to strengthen the protection, detection, response and recovery capabilities against ICT-related incidents and failures, ICT change management, etc.).
- *Reporting and threat intelligence* refers to the rules that will govern the reporting of ICT-related incidents (e.g. in particular on the level of ambition for streamlining existing rules), and the exchange of threat intelligence among financial institutions.
- *Testing* refers to the different tools and measures that financial institutions should employ to assess the effectiveness of their preventive, detection, response and recovery capabilities to uncover and address potential vulnerabilities in their ICT systems and ICT services (e.g. via stress tests or digital operational resilience testing).
- *ICT third party risk* refers to the direct oversight or indirect supervision (e.g. through application of outsourcing rules) of ICT TPPs and the authority(s) that will perform this activity.

	ICT risk management	***Reporting and threat intelligence***	***Testing***	***ICT third party risk***
"Do nothing" scenario	*Status-quo for EU financial services rules + NIS Directive*	*Status-quo for EU financial services rules + NIS Directive Voluntary threat intel*	*Based on national rules*	*Status-quo on outsourcing based on ESAs guidelines (indirect supervision)*
Option 1	*Capital buffer + NIS Directive*	*Same as "do nothing"*	*EU – wide resilience stress tests*	*Capital buffer*
Option 2	*Comprehensive EU rules in financial services legislation + NIS Directive*	*Comprehensive EU rules in financial services legislation + NIS Directive Voluntary threat intel*	*Comprehensive EU rules on digital operational resilience testing + mutual recognition of*	*EU oversight framework*

			testing results	
Option 3	*Comprehensive EU rules in financial services legislation* *+ out of NIS completely*	*Comprehensive EU rules in financial services legislation* *+ out of NIS completely* *Compulsory threat intel*	*Comprehensive EU rules on digital operational resilience testing* *+ cross-authority testing under ESAs coordination*	*New EU Authority (direct supervision)*

4.1. Do nothing: No change in the EU financial services regulatory framework

Under this scenario, the Commission will not propose any changes to the current EU regulatory framework governing digital operational resilience for the financial industry. Rules addressing operational resilience would continue to be set by current provisions in the EU financial services legislation, which as highlighted differ substantially across sectors, partly by the NIS Directive and its forthcoming review, as well as by national schemes that have emerged or could emerge in the future. In addition to the planned review of the NIS Directive, progressive harmonisation and alignment of ICT security and supervisory practices across the financial sector could take place on a voluntary basis through soft law measures (e.g. guidelines, recommendations) by the ESAs. Under this scenario, financial institutions would also continue to be encouraged to take into account international standards, principles and best practices issued by global standard setting bodies, which in due course may lead to changes to provisions in EU financial regulatory legislation.

For each of the main policy areas, no changes to the regulatory framework would entail the following:

a) **ICT risk management**: requirements on ICT risk would remain fragmented across sectoral and horizontal legislation. Such fragmentation is likely to remain also after a revision of the NIS Directive: Such a review can expand the personal and material scope of ICT risk requirements to further parts of the financial sector, but it cannot overcome fragmentation because of the continued interaction with fragmented sectoral legislation.

b) **Incident reporting and information sharing**: in the absence of EU regulatory action, financial institutions will remain subject to multiple reporting obligations that entail different timelines, reporting templates, authorities, thresholds, etc. In the same vein, competent authorities will continue to experience difficulties in monitoring ICT incidents and their impact upon the financial sector. Similarly to point a), a revision of the NIS Directive could expand the personal and material scope of incident reporting and information sharing, but it will not overcome the fragmentation of requirements, as requirements established by sectoral legislation will remain fragmented. Currently, cyber threat intelligence sharing is voluntary and only a limited number of financial institutions are taking part in such initiatives. Legal and regulatory barriers are often quoted as reasons for not engaging in threat intelligence sharing. Without any regulatory action, information sharing arrangements would remain limited and fragmented in the EU, thus missing the opportunity to create synergies that leverage in a collective manner financial institutions' individual knowledge and practical experience. Financial institutions' efforts to build up their defensive capabilities, threat detection techniques and mitigation strategies may then be less effective.[59]

[59] In February 2020, under the auspices of the ECB, the Euro Cyber Resilience Board for pan-European Financial Infrastructures took a first step by establishing a forum for strategic discussions between FMIs via the Cyber Information and Intelligence Sharing Initiative (CIISI-EU):

c) **Digital operational resilience testing**: no changes to the current EU regulatory framework implies that Member States will continue to develop and implement their own national testing frameworks. This will likely lead to increased multiplication and duplication of testing requirements on financial institutions with cross-border activities, and an increase of regulatory asymmetries due to the lack of mutual acceptance of testing results. The NIS Directive does not include specific requirements harmonising testing.

d) **ICT third-party risk**: with no changes in the regulatory framework, the arrangements and supervisory practices in applying the rules for financial institutions on outsourcing to ICT third party service providers (the *indirect* oversight), where they exist, will remain scattered. The Commission's ongoing work on standardising contractual clauses for outsourcing to cloud by financial institutions may improve the contractual position of financial institutions, however only in relation to one subset of ICT TPPs (cloud providers). Moreover, without binding regulatory principles, financial institutions will continue to face limitations and challenges to comply with and/or reinforce the regulatory framework on outsourcing (including the sub-outsourcing value chain). In addition, prudential supervisors will continue to lack the appropriate tools to analyse and oversee the impact of third party dependencies on the financial system. While the NIS Directive includes ex-post supervision of security requirements and incident reporting of cloud service providers, it is limited to only one subset of ICT TPPs, it does not deal with the oversight of all critical ICT TPPs when they provide their services to financial institutions, nor does it deal with outsourcing to such entities.

4.1.1. Overall assessment of the current state of play and how the problems would evolve

A progressive harmonisation of **ICT provisions** and **incident reporting** requirements across financial subsectors will not take place. While some financial institutions may upgrade their ICT security, this would happen only unevenly, and due to the interconnectedness of the financial system, the remaining financial institutions will continue to pose risks for all operators in the financial system. Risks for financial sector stability and integrity (see section 4.3.1 below for an estimation) would therefore not be mitigated substantially.

Similar considerations apply to the national rules and supervisory practices on the direct and indirect oversight of **TPPs**, which are expected to remain scattered across the different financial subsectors. Under this scenario, financial institutions and prudential supervisors would thus miss on the expected benefits (e.g. cost effectiveness, increased compliance with the regulatory framework, improved monitoring over the activities of ICT TPPs,) that a coherent EU oversight framework might entail.

Regulator sponsored **cyber resilience testing** is a relatively recent practice for the financial services industry, and financial institutions (mainly from the banking sector) are gradually implementing the different schemes on a voluntary basis. Without a coordinated EU approach in this area, cyber resilience testing would continue to be patchy and there would be no mutual recognition of testing results across different jurisdictions; also, it is unlikely that other

---

https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html. Such model may help catalysing similar initiatives, but it is too early to assess its impact.

financial subsectors beyond banking and market infrastructures would adopt such schemes on a meaningful scale, therefore missing out on the potential benefits, such as for example revealing vulnerabilities and risks, test defence capabilities and business continuity, increase trust of customers, suppliers and business partners, etc.

The **information sharing arrangements** and initiatives would not be incentivised and are likely to remain underdeveloped and scattered across the EU. There are important economic and social benefits that could be missed, such as strengthening defence capabilities to prevent incidents from happening, increase access to knowledge and resources for less prepared entities in the sector, sharing of resources to jointly procure cybersecurity services from IT security companies, etc.[60]

The forthcoming review of the NIS Directive might bring changes, among others in terms of expanding the scope of the directive and providing greater harmonisation of requirements. However, the current NIS Directive is focused on cyber security and is not explicitly addressing broader digital operational resilience issues, such as **testing**, **information sharing among peers**, **direct oversight of ICT TPPs** (with the exception of the ex post supervision of cloud service providers mentioned under letter d)) and **outsourcing** rules to such entities. Moreover, digital operational resilience risks are inherently linked to the broader set of risks financial institutions face (e.g. market risk, credit risk, liquidity risk, etc.). All these risks are embedded, to a greater or lesser extent, in the EU financial services legislation, and are continuously supervised by financial supervisors as part of their mandate. The Single Rulebook for financial services is the foundation of the EU single market in financial services both in the Banking Union and in the Capital Markets Union. A mere review of the NIS Directive, without adjusting supervisors' toolbox to protect financial stability and market integrity would not be sufficient to ensure fully coherent and harmonised rules for financial institutions, given the interlinks with the broader set of financial risks. Financial supervisors would not be empowered with an integrated European framework to perform their mandate, which is of particular relevance as a legal basis for supervisors established at EU level (e.g. banking under the SSM supervision).

Under this scenario, it is unlikely that streamlining ICT-related **incident reporting** and addressing overlapping requirements would be achieved. Given that these provisions are present in several pieces of EU legislation or supervisory practices (e.g. NIS Directive, PSD2, ECB incident reporting scheme, etc.), reviews of individual legislations would bring limited to no benefits in this regards. Similarly, in order to reduce single market fragmentation and enable cross-border acceptance of **testing** results, limited to no benefits are expected through individual reviews or no action taken at EU level.

Costs (direct, indirect, regulatory charges, administrative costs)

For financial institutions: financial institutions' digital operational resilience will continue to be governed by the different EU financial services legislation and partially by the NIS Directive, depending on how Member States have implemented that Directive. Institutions facing overlapping incident reporting on the same incident and multiple testing frameworks in several jurisdictions will incur high costs (for more details see section 4.3.1 below and section 3.7 of Annex 3).

[60] ENISA study on Information Sharing and Analysis Center (ISACs) - Cooperative models, (2018).

Under the "do nothing" scenario, financial institutions will continue to be bound by existing multiple **incident reporting** obligations. In this context, incidents will continue to be categorised differently due to diverse reporting requirements (e.g. different taxonomies, thresholds, etc.) and disparate methodologies that authorities use to collect data. Over time, such approach will generate increasing expenses in compliance costs and administrative burden.

The current absence of mutual acceptance of **testing** results across the Member States is likely to remain at the same levels and this may lead to additional costs, more administrative burden and additional regulatory misalignments.

In addition, even without any policy change, financial institutions are likely to face increasing costs in compliance and due diligence processes in the next years. Even today and in the absence of a uniform and comprehensive EU initiative, financial institutions voluntarily implement and update security measures or plan significant investment programmes in the next years. Some follow national or EU rules (e.g. EBA guidelines and Solvency II) or global standards (e.g. ISO, NIST,[61] etc.). Based on global and regional regulatory requirements and best practices, respondents to the public consultation mentioned to have developed their own policies, standards, and guidelines covering information security and risk, and will increase their spending on this front. However, they found it difficult to anticipate any quantification of such development of expenses (for more details see point 3.1 of Annex 3).

Threat intelligence sharing is considered a useful preventive practice in the cyber resilience toolbox of financial institutions, as it can help market participants to exploit the economies of scale generated by the network through an active sharing of information on possible threats. Under this scenario, financial institutions are subject to these costs (see section 4.3.1 below for a detailed estimation of these costs) only when they engage in such initiatives on a voluntary basis, and their engagement is proportional to the level of available resources.

For supervisors: Over the last few years, several prudential supervisors have been increasing their resources dedicated to IT supervision. Under this scenario, the overall costs related to supervision, reporting and enforcement borne by national competent authorities as a result of monitoring ICT-related activities in each national jurisdiction are likely to remain and further increase as supervisors may upgrade their systems unevenly on a voluntary basis. On average, according to supervisory data and Commission's calculations, it is estimated that currently around 5-10% of the total FTEs dedicated to supervising financial institutions are assigned to IT supervision.

Overall, the ongoing **COVID-19** crisis is likely to further accentuate many of the costs highlighted above. The crisis has so far illustrated the benefits of digital finance in ensuring access to financial services on a remote basis. It is therefore likely that financial services policy at various levels will in the near future focus on further digitalising finance. This will put further emphasis on strengthening digital operational resilience. Hence, in the absence of a coherent response at EU level, national/sectoral actions are likely to proliferate, thus accentuating the costs outlined above.

[61] NIST here refers to the cybersecurity framework developed by the National Institute of Standards and Technology, a unit of the U.S. Commerce Department.

4.2. Option 1: Strengthening financial institutions' ability to absorb losses stemming from lack of digital operational resilience

EU financial services legislation is governed by a set of sectoral provisions on risks (e.g. market risk, operational risk, credit risk, liquidity risk, etc.). One of these risks is operational risk and it covers the risk of losses resulting from "inadequate or failed internal processes, people and systems or from external events".[62] For banks and insurance services, for example, these provisions translate into capital charges. This quantitative approach is in line with international regulatory measures to address risks through capital charges/buffers. For instance, the Basel Committee on Banking Supervision (BCBS) has recently revised the operational risk framework by addressing the risks with increased capital. Under this option, strengthening the digital operational resilience in financial services would be achieved by amending the different provisions on operational risk in the EU financial services legislation and partly by the review of the NIS Directive.

In contrast to the other options, this option – in addition to the review of the NIS Directive – follows a purely quantitative approach targeted at increasing the capital charges and loss absorption capacity for operational risks. This reduces the financial risk (of default) from an operational risk event. Setting capital aside to cover a potential risk represents a cost for the financial institution. Capital charges should accordingly incentivise financial institutions to reduce their exposure to the underlying risk to the extent possible.

Under this option:

a) **ICT risk management**: first, the current operational risk framework would be amended by introducing a specific loss event type on ICT risk. Second, a new and specific capital buffer for ICT risk would be created and it will sit above the capital provisions for operational risk. The calibration of this capital buffer would be based on historical data on losses due to ICT-related incidents.

b) **Incident reporting and information sharing**: Streamlining and improving incident reporting to financial supervisors would not be addressed under this option. Financial institutions would be required to report losses stemming from ICT-related incidents and provision the specific capital buffer based on past losses resulting from ICT-related incidents. The level of this specific capital buffer would very likely be higher as compared to the current rules on operational risk. The sharing of cyber threat intelligence will continue to be voluntary and limited to the financial institutions currently participating in such initiatives.

c) **Digital operational resilience testing**: under this option, the digital operational resilience of financial institutions would be assessed through stress testing the specific capital buffer for ICT risk. For banks, the existing EU-wide stress tests coordinated every two years by EBA would be used. These tests assess how resilient banks are to economic shocks. The specific capital buffer for ICT risk would be included in the methodologies and scenarios of the EU-wide stress test. For other financial institutions, a similar stress testing exercise focused on ICT risks would be developed by the ESAs and run in collaboration with the national competent authorities.

[62] Basel Committee on Banking Supervision (BCBS), Principles for sound management of operational risk (PSMOR).

d) **ICT third-party risk**: under this option, a dedicated capital buffer for exposure to ICT TPPs would be set in the legislation. This capital buffer would aim to strengthen the financial resilience of financial institutions by increasing the loss absorption capacity from operational incidents stemming from ICT TPPs, and, similarly to capital charges more broadly, incentivise financial institutions to reduce those risks.

4.2.1. Assessment of the impact

Benefits

Reduce the risk of financial instability: only one (i.e. *strengthen the overall level of digital resilience of the financial sector*) out of the six specific objectives in Table 2 would be partially achieved.

The overall resilience of the financial sector would be enhanced through increasing the loss absorption capacity of some financial institutions. Some benefits would be achieved compared to the "do nothing" scenario, as better capitalised financial institutions would have more financial resources to absorb the impact of ICT-related incidents. Furthermore, additional benefits could result over time from lower capital charges if financial institutions take actions to improve their resilience, as less incidents would translate into lower capital provisions. This may accordingly improve system resilience over time. However, this option would not be equally effective for all financial sectors, as evidenced by recent incidents at, for instance, Bank of Valetta and Equifax. In these cases, the impact on capital was significant and clearly exceeded any additional capital charges which could reasonably be put on financial institutions. For Bank of Valetta, the €13 million that were subject to the cyber incident[63] represented approximately one third of its minimum capital requirements for operational risks (in accordance with Article 438 (c) to (f) of CRR).[64] In the case of Equifax, the estimated losses of around $1.38 billion exceeded by far the minimum capital requirements for operational risks and accounted to approx. 40% of their total capital, and to around 20% of their total assets.[65] In addition, for the first time ever, there was a change of rating outlook for Equifax due to a cyber breach,[66] which can lead to additional costs such as increase in the costs of borrowing and access to capital markets.

In terms of financial supervisors' access to information on **ICT-related incidents**, this option would bring no improvement. Compared to the current rules, and as such, no benefits are expected compared to the "do nothing" scenario. From the perspective of financial institutions, the voluntary exchange of threat intelligence across the financial sector would likely remain at the same level as compared to the "do nothing" scenario. The benefits of incentivising the exchange of threat intelligence in the financial sector would not be achieved.

Under this option, **ICT TPPs** would continue to be subject to an *indirect supervision* performed by supervisors over the supervised financial institutions through the different

[63] It should be noted that the €13 million that were initially stolen were finally recovered, according to media: https://www.reuters.com/article/us-bank-valetta-cyber/cyber-attack-on-malta-bank-tried-to-transfer-cash-abroad-idUSKCN1Q21KZ.
[64] 2019 Annual Report of Bank of Valetta, https://www.bov.com/documents/bov-annual-result---2019.
[65] According to media reports, the total estimated losses for Equifax were about 1.38 billion USD. See: https://www.securitymagazine.com/articles/91573-equifax-settles-2017-data-breach-for-138-billion. For the annual accounts, see https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2017-annual-report.pdf
[66] https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html.

written agreements used in outsourcing arrangements. In this context, financial institutions would continue to face challenges in assuring compliance with the regulatory framework when certain functions are outsourced or further sub-outsourced to ICT TPPs, and thus there would be no expected benefits as compared to the "do nothing" scenario. In addition, there will be no *direct oversight* over ICT TPPs under this option, except that cloud computing services that are subject to the current rules of the NIS Directive, would continue to comply with the security and notification requirements therein. Therefore, there are no expected benefits as compared to the "do nothing" scenario.

Reducing administrative burden and increase supervisory effectiveness: only one (i.e. *reduce single market fragmentation and enable cross-border acceptance of testing results*) out of the two specific objectives in Table 2 would be partially achieved.

Under this option, there will be no action taken to streamline the ICT-related **incidents reporting** and the overlapping requirements would not be addressed. Therefore, no expected benefit as compared to the "do nothing" scenario.

The EU-wide stress tests would achieve the objective of reducing single market fragmentation and enabling cross-border acceptance of testing results. However, it should be noted that financial institutions would not be required to build up preventive and resilience capabilities that enable them to better identify and assess ICT vulnerabilities they are exposed to. Therefore, from this perspective, limited benefits are expected under this option as compared to the "do nothing" scenario.

Finally, the objective of **increasing consumer and investor protection** would be partially achieved at higher costs for the current shareholders/prospective investors of those financial institutions that would have to strengthen their capital.

Costs (direct, indirect, regulatory charges, administrative costs)

For financial institutions: provisioning for a new capital buffer on ICT risk and TPPs exposures would entail greater compliance costs to raise additional capital of a high quality, and an increase in own funds would require financial institutions to maintain the level of provisions up to a certain minimum level on a permanent basis. Under this option, the capital buffer would nevertheless not lead to such significant capital increases that it would be out of proportion with the policy positions taken by the international supervisory community. For example, the recent finalisation of the international Basel III accord on bank supervision, which the Commission remains committed to implement, would lead to an average increase of 23,6% of a credit institution's total capital in the EU[67]. In comparison, tackling digital operational resilience by a quantitative approach would not lead to capital increases which would be completely out of proportion. In order to further illustrate the scale of the potential additional levels of capitalisation under this option, we could use as proxy the amount of estimated losses incurred by financial institutions in a specific ICT related incident and express it as a percentage of the institutions' total capital. Table 3 below gives an indication of the potential additional levels of capitalisation that could be expected under this option. These levels are wide-ranging and further calibration is needed.

Table 3 - potential additional levels of capitalisation under option 1

[67] https://eba.europa.eu/eba-updates-estimates-impact-implementation-basel-iii-and-provides-assessment-its-effect-eu-economy

Financial institution	Estimated costs of past incidents[68]	Total capital	Estimated costs of past incidents as percentage of total capital
Equifax	$ 1,38 billion	$ 3,2 billion	42,6%
TSB Bank	£ 330 million	£ 1.879 million	17,6%
Capital One	$ 150 million	$ 58 billion	0,3%
Banco de Chile	$ 10 million	$ 4,08 billion	0,2%

Source: Financial institutions' annual accounts, press review and Commission's calculations

In addition, there will be other direct costs associated with the process of regular reporting on the capital buffer, as well as with adapting the IT systems. Financial institutions would face direct and administrative costs associated with extending the stress testing exercises to other financial sectors, beyond banking.

For supervisors: the EU-wide stress test exercise for banks involves several actors in the EU financial sector (e.g. staff from ESRB, NCAs, ECB, European Commission, etc.), is quite resource intensive and is prepared over a period of two years (e.g. design of methodology, scenarios, data collection, quality checks, running the exercise, publication of results, etc.). The exercise is coordinated by the EBA, with 7 FTEs directly involved in this process,[69] while the total FTEs involved in the entire exercise amount to at least 250 FTEs,[70] with a tendency to increase the number of staff over time. By including the envisaged capital buffer for banks, a marginal increase of around 5-10% in the costs is estimated.[71] However, developing an EU wide stress test on ICT risk that goes beyond banking and covers all financial sectors would entail significant costs for the securities markets and insurance prudential supervisors. It would require specialised technical expertise (e.g. modelling experts, examiners, ICT and TPPs risk specialists, considerable time to develop capable testing resources, etc.). It is estimated that the amount of direct costs would be in the range of 25 to 50 FTEs.[72]

4.2.2. Overall assessment of the option

The main advantage of this option is that it provides for limited changes to existing EU financial services legislation. These limited amendments would be targeted to introduce a new /separate type of loss event in the operational risk frameworks coupled with a new specific capital buffer for ICT risk and TPPs exposure. Another advantage is that over time, it may increase system resilience if financial institutions implement measures to increase their digital

[68] See: https://www.securitymagazine.com/articles/91573-equifax-settles-2017-data-breach-for-138-billion, https://www.theguardian.com/business/2019/feb/01/tsb-computer-meltdown-bill-rises-to-330m, https://www.reuters.com/article/us-capital-one-fin-cyber/capital-one-says-information-of-over-100-million-individuals-in-u-s-canada-hacked-idUSKCN1UO2EB and https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075.

[69] European Court of Auditors, 2019 Special Report on EU-wide stress tests for banks: unparalleled amount of information on banks provided but greater coordination and focus on risks needed. https://www.eca.europa.eu/Lists/ECADocuments/SR19_10/SR_EBA_STRESS_TEST_EN.pdf.

[70] Basel Committee on Banking Supervision, "Supervisory and bank stress testing: range of practices", December 2017, https://www.bis.org/bcbs/publ/d427.pdf.

[71] This estimation is based on the assumption that between 5 to 10% of the total EU-wide stress tests FTEs are dedicated to operational risk related issues (including ICT risk).

[72] This estimation is based on the assumption that between 5 to 10% of the total EU-wide stress tests FTEs are dedicated to operational risk related issues (including ICT risk). The range of 25 to 50 FTEs results from applying this percentage to the total FTEs for the EU-wide stress tests, and then multiply by two to account for both the securities markets and insurance sectors.

operational resilience and reduce ICT-related incidents based on which the provisioning will be calculated.

The main disadvantage of this option is that it will have only limited effects on increasing the operational, as opposed to financial, resilience of the EU financial sector, as provisioning more capital to cater for losses stemming from ICT-related incidents would be an insufficient measure and, while firms may be incentivised to take measures to improve their resilience in order to reduce their capital requirements, there is no clarity on the nature of these measures or the degree to which firms will actually strive to adopt such measures (or just accept the capital charge). This option is accordingly rather costly, as evidenced in the above assessment, with very limited benefits in terms of effectiveness. This high cost is particularly relevant in the current context of COVID-19. Overall, this option would address to a very limited extent objective 1 and 3, but not objective 2.

Note that this option would not be in line with ESAs joint technical advice, where the ESAs recommended the Commission to make legislative changes targeted at *qualitative* measures in different areas, for instance introducing specific requirements in the legislation on operational resilience to support good and consistent ICT risk management across the financial sector.

Effectiveness, efficiency, coherence

This option would be the least effective, as it would achieve only two of the eight specific objectives of the initiative, and that would imply that the problems identified would persist or even magnify. The quantitative measures envisaged under this option would entail important costs for financial institutions, as capital charges represent one of the most costly regulatory measures. This option would also require more clarity and coherence with the existing horizontal EU framework (e.g. NIS Directive).

Impact on stakeholders[73]

Based on the above assessment, the following table summarizes the benefits and costs of the option for each category of stakeholders, while the vertical arrows present the estimated impact for these stakeholders. Financial institutions would benefit from partially strengthening their overall digital operational resilience and consumers/investors would be slightly more protected from negative repercussions stemming from operational losses. However, this comes with significant costs for the supervisors and financial institutions.

	Consumers/investors	Financial institutions	ICT TPPs	Supervisors
Benefits	↑	↑	≈	↑
Costs	↑	↑↑↑	≈	↑↑↑

4.3. Option 2: A digital operational resilience act for the financial sector

Under this option, the Commission would propose a comprehensive framework addressing in a consistent manner at EU level the digital resilience needs of all regulated financial

[73] Throughout the document, stakeholders are grouped in categories slightly different from the traditional categories of stakeholders to reflect the main actors that will be impacted by the new rules.

institutions, as opposed to 27 national regimes or to different EU pieces of financial legislation. In contrast with Option 1 – which relies on the existing quantitative approaches to provisioning against operational risks by means of increasing firms' loss absorbing capacity – Option 2 would strengthen the qualitative dimension of the operational risk framework by building a proper *digital operational resilience core requirements (the "core requirements")*.

Under this option, *the core requirements* in the initiative would apply across the financial sector. When defining the *core requirements* across the four main areas, the principle of proportionality would apply both across the subsectors, but also within each subsector, taking into account, where relevant, specific needs arising for specific categories of financial institutions, as well as their business models, size, risk profile, systemic importance, etc. For instance, in terms of **ICT risk management** requirements, only insignificant changes would be required for payment service providers, central counterparties or central securities depositories, as these institutions are already subject to rigorous requirements. More significant changes of requirements would be envisaged for other subsectors like banking, asset managers, insurers, etc. In terms of the type of institutions, bigger and systemic institutions would be subject to more stringent requirements, while for smaller institutions these requirements could be less exhaustive. In terms of **incident reporting**, existing disparate and overlapping requirements would be streamlined, as well as new requirements introduced for those subsectors that are currently not subject to such rules. Not all financial institutions would be equally affected by these rules, as materiality thresholds, time frames to report ICT-related incidents, etc. would be calibrated to capture major incidents. For instance, these rules could be more relevant for significant financial institutions and impact less on smaller entities. Financial institutions would be also required to **test** their preventive and responsive capabilities. This would be more demanding for significant financial institutions (e.g. big banks, stock exchanges, CSDs, CCPs, etc.) At the same time, testing would be also more relevant for some subsectors with a core systemic role (e.g. payments, banking, clearing and settlement), and less relevant for other subsectors e.g. asset managers, credit rating agencies, etc. Finally, the rules on **third party risk** would cover two main areas: strengthened requirements on outsourcing to ICT third party providers, and a direct oversight of the activities of ICT TPPs. The detailed calibration of the proportionality elements of the measures will depend on financial institutions' systemic relevance and size. For more specific details on the main elements of *the core requirements* and how it would affect the different financial subsectors, see Annex 4.

Financial subsectors under the scope of the NIS Directive would remain subject to the NIS Directive and its *lex specialis* exemption would continue to apply. As a consequence, the substantive requirements of the NIS Directive would not be applicable to them. They would however remain associated with the NIS 'ecosystem provisions' (e.g. Cooperation Group, CSIRTs network) through a specific article in the new act. The association would materialise via, for example, the exchange of information and cooperation between financial supervisors and the NIS designated authorities or the participation of financial supervisors in the NIS Cooperation Group.

Under this option:

a) **ICT risk management**: The digital operational resilience would be rooted in rules implementing core requirements for a sound ICT risk management framework, in line with the joint ESAs technical advice. All financial institutions would be required to have in place an ICT risk management framework developed on key common principles that are risk-based and allow for a proportionate application. The ICT risk

management cycle would be composed of several stages designed to identify ICT risk, detect threats and vulnerabilities, protect against them, respond to them, recover and learn from disruptions and, finally, share threat intelligence with other peers.[74]

b) **Incident reporting and information sharing**: communication on ICT-related incidents (ex-post reporting to competent authorities) would be enhanced and extended to those subsectors currently not subject to such rules. Current rules, which are either disparate or overlapping, would be deleted in every relevant directive/regulation across the financial sector, be they in level 1 or level 2 acts. Financial institutions would follow a single incident reporting scheme that would be set out in the new act, with one set of criteria to qualify what is a "major" ICT-related incident, one template, one deadline, and one competent authority to report to, in line with the joint ESAs technical advice. Because the *lex specialis* clause would be better explained in the new act, leaving no room for national interpretation and divergence, the current double reporting of the same incident to different competent authorities would be eliminated. Instead, the competent authority receiving the reports would be required explicitly to exchange the information with other authorities within and across Member States, where relevant.

   Under this option, the enhanced reporting of ICT-related incidents would be complemented by a voluntary scheme encouraging communication on threats (ex-ante information sharing between financial institutions, and involving relevant authorities where applicable). Information sharing on key lessons and main vulnerabilities in a trusted environment would enhance awareness and readiness to react and thus render the financial sector more stable. Information sharing will have to be compatible with existing EU law, e.g. the GDPR that also contains specific safeguards allowing for information sharing in the interest of security (one of the "legitimate interests" under Article 6(1)(f)).

c) **Digital operational resilience testing**: a proportionate resilience testing framework that so far has been designed at national level would be replaced by harmonised EU rules. More advanced testing (for example threat led penetration testing) would be required only for significant financial institutions, in line with the joint ESAs technical advice. Testing results would be mutually recognised across the national competent authorities in the EU. The new act would empower the ESAs to develop rules to determine cyber maturity, as well as guidelines for TLPT testing, based on e.g. TIBER-EU.

d) **ICT third party risk**: an enhanced monitoring of risks stemming from ICT TPPs would be built upon two elements: heightened outsourcing rules and oversight tools for supervisors in relation to ICT activities of TPPs when they provide their services to financial institutions, which in the case of cloud service providers would complement the direct ex post supervision of security requirements and incident reporting under the NIS Directive. The new act would grant supervisors certain powers and tools for monitoring systemic risk resulting from ICT TPPs, identifying points of failure, concentration risk and risk transmission channels, in line with the joint ESAs technical

[74] In terms of legal drafting, first, the provisions on operational risk that already exist in the current acquis would be maintained, but any references to ICT risk thereof would be deleted and replaced by an amendment specifying that the qualitative aspects of the digital component of operational risk are to be found in the new act. That way, the cross-reference between each piece of legislation in the financial sector acquis and the horizontal act on digital operational resilience would be clearly established, avoiding possible loopholes and legal uncertainty. Second, in those legal acts that do not contain explicit provisions on operational risk (e.g. UCITS, AIFMD, CRAR, etc.), a similar amendment would be made under the section dealing with risks, to make sure the risk landscape is complete for every single financial subsector.

advice. These new powers and tools for prudential supervisors would include e.g. recommendations, enhanced inspection rights, pooled audits, etc. Taking into account that large critical ICT TPPs operate cross-border, regulatory oversight could be achieved via cooperation agreements, joint inspections and exchange of information.

4.3.1. Assessment of the impact

Benefits

Reduce the risk to financial sector stability and integrity: all six specific objectives detailed in Table 2 would be achieved under this option.

The harmonisation envisaged under this option would address in a comprehensive manner **ICT risks** across the financial sector. The rules would lift up the level of the core requirements on digital operational resilience across the financial subsectors by enhancing the protective and responsive capabilities of financial institutions against ICT-related incidents. This would in turn, address the vulnerability outlined in section 1.2 (cf. figure 2), i.e. reduce the risk of a cyber incident quickly spreading across financial markets and jurisdictions. It will also secure the operating environment for all financial market participants even in a strongly interconnected environment, and thus increase the overall digital operational resilience of the EU financial sector. Almost all respondents to the public consultation agreed that *all* financial entities should have in place an ICT risk management framework based on key common principles and allow for a proportionate application.

Under this option the main expected benefits would result from the likely contribution of a comprehensive digital operational resilience framework to reduce the risk of financial sector stability and integrity and to 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 $45 billion to $654 billion for the global economy in 2018.[75] 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[76], this would imply costs in the range of $2 billion to $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. As evidenced by the ESRB and confirmed by the responses to the public consultation, estimating the cost of cyber incidents in a more detailed manner is extremely difficult for two main reasons: (i) not all cyber incidents are reported, and (ii) even for those reported, it is often not clear to what extend the figure includes direct losses (e.g. loss of revenue, funds stolen, repair costs, etc.) and indirect losses (e.g. loss of reputation, legal costs and fines, etc.).

Financial supervisors would be immediately and directly notified by the financial institutions themselves of all major ICT-related incidents they experienced. This direct **reporting** contributes to achieving the objective of enabling financial supervisors' access to information on ICT-related incidents. The information that supervisors will receive would feed into the overall supervisory process as part of their mandate, and could lead in some instances to

[75] ESRB report *Systemic Cyber Risk* and https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html.
[76] According to IMF data, the EU economy represent approx. 21% of the global economy. Source: IMF - https://www.imf.org/external/pubs/ft/weo/2016/02/weodata/index.aspx.

additional actions taken by financial supervisors such as e.g. increased capital charges, on-site inspections, and even in sanctions, etc. Under this option, financial supervisors would also be obliged to pass on this information to non-financial authorities. Notifications would accordingly also reach other authorities outside the financial sector (NIS authority, data protection national authority, law enforcement authorities for incidents of criminal nature).

Harmonised basic and advanced **testing** would ensure that financial institutions assess on an ongoing basis or frequently, respectively, the effectiveness of their preventive and resilience capabilities to identify, repair and mitigate ICT vulnerabilities that could otherwise be exploited by malicious actors. The main benefits for financial institutions would come from an increased detection of unknown vulnerabilities and risks in their systems and digital assets, enabling them to take timely actions for increasing resilience against possible disruptions. The majority of respondents to the public consultation call for EU legislative changes going in these directions (see Annex 3).

Under this option, voluntary sharing of vital **threat intelligence** in the financial sector via platforms would be promoted/encouraged, and thus it is very likely that it would no longer be an exception, but become the common practice; by creating trusted communities to discuss cybersecurity threats and best practices, the main benefits for financial institutions would be an increased capacity to leverage their collective knowledge and experience to address the threats ahead of them and make informed decisions about their defensive capabilities, threat detection techniques and mitigation strategies. The majority of respondents to the public consultation agree that the EU should play a role in supporting and promoting the voluntary information sharing as it would help reduce information asymmetries across jurisdictions, and foster coordination, communication and cooperation among financial institutions and competent authorities (if they collaborate on such platforms) (for more details see point 3.5 of Annex 3).

When it comes to **ICT third party risks**, the existing set of EBA guidelines on outsourcing are only applicable to banks and payment service providers, but not to (re)insurance or securities markets entities. In addition, given that the EBA guidelines are applied on a *comply or explain* basis, some competent authorities were non-compliant by the entry date into force, while others already announced they will not comply with some of the principles.[77] EIOPA has also published a set of guidelines on outsourcing to cloud service providers, which are expected to entry into force in January 2021. Under this option, the currently limited and scattered outsourcing rules in financial legislation would be strengthened by elevating and substantiating the main principles in the EBA/EIOPA Guidelines on outsourcing into the new act. Such principles would be imposed as obligations on all financial institutions. This would provide them with a coherent set of rules on managing the risks associated to outsourcing to ICT TPPs. In this way, financial institutions would have a comprehensive framework with specific provisions against which they would need to ensure compliance of their contractual relationship with ICT TPPs. To reflect these legal requirements and guidelines in their contracts with ICT TPPs, market participants could e.g. choose to deploy the Commission's forthcoming Standard Contractual Clauses. The main benefits for financial institutions would result from an increased ability to enforce the contractual rights in order to ensure ICT TPPs' compliance with the regulatory framework. This would also alleviate some supervisory concerns around operational risks which, although originated at a third party (or further in the

[77] See EBA Compliance table for more details: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

sub-outsourcing chain), have direct consequences on the actual performance of financial institutions.

Under this option, and in the absence of a sector-agnostic horizontal digital oversight authority (e.g. through another Union act), financial supervisors would have direct oversight over the activities of ICT TPPs, thus ensuring better micro and macro-prudential scrutiny over risks that may arise outside the financial sector. As evidenced before in section 2, almost 60% of the companies experienced a data breach caused by a third party provider according to the Ponemon Institute. The Institute of International Finance (IIF)[78] highlights that one of the risks to financial stability stems from the digital transformation that creates single points of failure. According to industry research[79], around 70% of the global market for cloud (i.e. infrastructures as a service and platform as a service) lies in the hands of four cloud service providers, all of them non-European. An overwhelming majority of respondents to the public consultation supported the introduction of an oversight framework for critical ICT TPPs (for more details, see point 3.4 of Annex 3).

Reducing administrative burden and increase supervisory effectiveness: both specific objectives detailed in Table 2 would be achieved under this option.

ICT-related incident reporting would be streamlined, so overlapping and duplicative requirements would be deleted and compliance costs and burdens be alleviated. In their replies to the public consultation, almost all stakeholders called for a harmonised taxonomy of reportable incidents, reporting templates and timeframes, and materiality thresholds. One respondent estimated the impact of such overlapping requirements to be around 2% of their cybersecurity budget. The expected benefits would the savings from eliminating the costs of overlapping and duplicative reporting. As illustrated in section 2.1.2, one of the subsectors that is facing multiple reporting obligations of the same incident is banking. If we take as a reference the 2% costs mentioned by the respondent, and apply it to 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.[80]

Also, fragmentation would be eliminated thanks to a single set of testing rules applicable to all EU financial institutions. The expected benefits would be even more relevant for cross-border financial institutions as they would need to comply with a single set of advanced testing requirements (e.g. TLPTs) and incur testing costs in one jurisdiction only. According to supervisory data and Commission's calculations, it is estimated that in the absence of a coherent testing framework and mutual acceptance of testing results, cross-border financial institution could be subject to a range of 2 to 5 similar tests in different Member States. Respondents to the public consultation indicated that costs for such tests are in the range of €250-500.000, depending on the scope. Therefore, the potential cost savings could be estimated in the range of €250.000 to 2 million per cross-border financial institution. To

[78] https://www.iif.com/portals/0/Files/private/32370132_cloud_computing_in_the_financial_sector_20180803_0.pdf.
[79] https://www.srgresearch.com/articles/amazon-microsoft-google-and-alibaba-strengthen-their-grip-public-cloud-market.
[80] According to media reports and Commission's calculations, the annual IT budget of the top 6 EU banks (i.e. BNP Paribas, Credit Agricole, Deutsche Bank, Societe Generale, Banco Santander, ING) is estimated at around 24 billion EUR. A survey by Deloitte and FS-ISAC, shows that banks, insurers, investment management firms and other financial services companies spend anywhere from 6 to 14% of their information technology budget on cybersecurity, averaging 10%. The estimated range of €29 to 68 million is calculated by multiplying the 2% with the estimated annual IT budget of the top 6 EU banks (i.e. €24 billion), and with the range of 6 to 14% of cybersecurity share in the total IT budget.
Source: https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html.

illustrate the scale of savings in the banking sector where, according to ECB[81] and SRB[82] data, around 44 banking groups are undertaking cross-border activities in the EU, the total expected benefits could range between €11 and 88 million.[83]

Under this option, the objective of **increasing consumer and investor protection** would be also achieved. A strengthened digital operational resilient EU financial sector would indirectly benefit both consumers and investor, as they would be better protected from suffering the consequences of ICT-related incidents occurring at financial institutions. It is very likely that their trust in the financial sector would accordingly also increase.

Costs (direct, indirect, regulatory charges, administrative costs)

For financial institutions: the one-off adjustment costs, represented by investments in IT systems and a general improvement of qualitative ICT risk requirements, are not possible to quantify given the wide divergence in banks' legacy systems, their current level of preparedness and resilience (e.g. policies, controls, procedures), etc. However, they would be higher than under the previous options. 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, according to media review and Commission's calculations, the top 4 EU banks[84] have announced a total annual spending of around €1.1 billion on cyber security over the next years.

In terms of recurring costs, a survey by Deloitte and FS-ISAC[85] shows that on average banks, insurers, investment management firms and other financial services companies spend between 6% and 14% of their IT budget on cybersecurity, with an average of 10%. While at first sight, these investments seems to be an important part of their IT budget, in terms of revenues, they account to a range of between 0.2% and 0.9% of the total revenues, with an average of about 0.3%. While it is impossible to estimate the recurring costs of a general improvement of qualitative ICT risk requirements, it could be estimated that bringing ICT requirements up to a decent standard for all financial institutions would mean that institutions which have spending below the average would have to bring this up to the average. Another survey by Deutsche Bank[86] provides a breakdown on how much of the IT spending is dedicated to cyber security by financial institutions. On average, around 10% of financial institutions are below the 6%-14% range mentioned above. Taking into account the total number of entities operating in the EU financial sector[87], it could be therefore estimated that around 2100 financial institutions would be affected by the initiative, and would need to make additional investments of up to 5% of their IT budget to reach the lower bound of the average. However, these recurring implementation costs in practice are expected to be much lower for both big

[81] https://www.bankingsupervision.europa.eu/banking/list/who/html/index.en.html
[82] https://srb.europa.eu/sites/srbsite/files/23_december_2019_list_of_other_cross_border_groups.pdf
[83] The estimated range of €11 to 88 million is calculated by multiplying the number of banks (i.e. 44), by the amount of savings resulting from performing one single test instead of 2 to 5 tests. This translated into potentially up to 1 test less for the lower bound, and up to 4 tests less for the upper bound.
[84] Source: media review and Commission's calculations, based on data reported for BNP Paribas, Credit Agricole, Societe Generale and Banco Santander.
[85] https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html.
[86] https://www.db.com/newsroom_news/Deutsche_Bank_Investor_Report.pdf
[87] According to the impact assessment accompanying the review of the European Supervisory Authorities, (SWD(2017) 308, there are around 2,666 insurance undertakings, 1,573 IORPS, 2,500 Investment management companies, 350 Market infrastructures (such as CCPs, stock exchanges, systemic internalisers, trade repositories and MTFs), 45 CRAs; and 5,665 Credit institutions, 5,934 Investment firms and 2,500 Authorised payment institutions and electronic money institutions. This sums up to approx. 21.233 entities.

and smaller financial institutions. This is due to the fact that big financial institutions have already increased their spending on ICT and cyber security, while for smaller institutions the costs are expected to be lower as proportionality would apply in calibrating the measures. Finally, those financial institutions which are currently at suboptimal levels of digital operational resilience, could expect to incur higher recurring costs.

On **testing**, for those financial institutions which are not participating in TLPTs today but would be required to do so in the future, we estimate that under this option around 100 financial institutions[88] would be subject to TLPT, and they would be subject to additional costs. Costs of financial institutions' participation in testing are in the range of €250-500.000 per test, depending on the scope. In their technical advice, the ESAs estimate the costs of threat led penetration testing to amount to a range between 0.1% and 0.3% of the total ICT budget. Therefore, we could estimate that the total costs for testing the 100 financial institutions under this option would be in the range of €25 to €50 million. These costs will have to compared to the cost reductions due to the mutual recognition of testing, for financial institutions which are currently may be subject to several cyber resilience testing frameworks implemented in different Member States, and this is particularly relevant for those operating cross-border, as evidenced by the responses to the public consultation (see above; for more details see point 3.3. of Annex 3). Overall, cost associated to TLPTs are high, but lower than under the "do nothing" scenario where an uncoordinated increase of TLPTs with limited cross-border recognition would impose duplicative costs for cross-sector financial institutions.

The costs for financial institutions' participation in **threat intelligence sharing schemes** are wide-ranging and vary depending on the type of initiative, sometimes they are also based on entities' assets or revenues, and may include membership fees (e.g. from basic to premium membership), travelling costs, staff deployed, IT costs for the installation and set-up of an intelligence sharing platform, etc. On average, these costs which are recurring on a multi-annual basis range between €1.000 and €50.000, plus 1 to 3 FTEs. Under this option, participation for financial institutions would be encouraged but still remain voluntary, therefore no additional costs are foreseen as compared to the baseline.

Costs in relation to **incident reporting** would be drastically reduced (see above, under benefits) under this option due to no reporting under the NIS Directive and no double reporting to the national supervisor and the SSM for significant banks. However, there would also be new costs (e.g. additional FTEs, setting up IT systems, developing internal templates, etc.) for those financial institutions that are not so far subject to any incident reporting and will have to report ICT related incidents. The number of reported incidents would very much depend on the proportionality of the future rules and the calibration of materiality thresholds that would trigger reporting (e.g. major incidents). According to industry data[89] and Commission's calculation, it is estimated that on average, the one-off costs for a big European bank for developing an internal template for incident reporting would amount to approx. €9.000. Under this option, we can estimate the total additional one-off costs for financial

[88] According to the impact assessment accompanying the review of the European Supervisory Authorities, (SWD(2017) 308, there are approx. 21.233 entities operating in the EU financial sector. If we assume that on average around 1% of them are significant in terms of e.g. their size, cross-border activity, their economic importance for the EU or national economy, etc., this results in around 200 entities. Furthermore, we estimate that at least 50% of these institutions are already being tested under different frameworks, which leaves us with around 100 untested entities.

[89] These estimations are based on a limited survey to a few big European banks, and thus should be considered as a limited representation of the (whole) European banking sector.

institutions in the range of €9 and €18 million[90] and recurring costs for managing incidents and reporting (e.g. classification of incidents, regulatory scouting, updating templates, etc.) in the range of €18 to €36 million[91].

For ICT TPPs: costs would be higher than under the previous options, as they would have to adopt organisational changes to allow for the oversight of their operations. However, these costs would remain manageable, especially if a horizontal, sector-agnostic supervision on ICT TPPs emerges in the future. According to industry data and Commission's calculation, it is estimated that on average, the staffing costs for an ICT TPPs that would be subject to a direct oversight by financial supervisors would be in the range of 2 to 6 FTEs. At the same time, TPPs would see a reduction in the costs to deal with a multitude of requests for access to information, audit, etc. by numerous financial institutions prompted by their supervisors.

For supervisors: the current costs for supervisory authorities associated to ICT supervision are between 5% and 10% of the total IT supervision staff. Under this option, a marginal increase in FTEs could be expected, due to the additional tasks supervisors would have to deal with (e.g. including additional reporting of incidents). For instance, for those supervisory authorities that would take part in the direct oversight of ICT TPPs (e.g. cooperation agreements, joint inspections and exchange of information), the estimated increase in FTEs could fall in the range of 1 to 5 FTEs for the leading authority, and around 0.25 FTEs for the participating authorities. On the other hand, supervisory authorities that would not participate in the oversight arrangements of ICT TPPs, would still benefit from the outcome of such oversight (e.g. financial institutions under their direct supervision would use the services and products of the overseen ICT TPPs). In addition, as a result of the direct supervisory oversight of ICT TPPs, the costs associated with the indirect oversight for financial institutions would be significantly reduced.

4.3.2. Overall assessment of the option

The main advantage under this scenario is that a comprehensive framework on digital operational resilience would be very effective in improving the digital operational resilience of the financial sector. It would ensure full clarity and coherence within the Single Rulebook. It would also make the interaction with the NIS Directive and its review clearer and more coherent. It would also bring clarity to financial institutions on the different rules on digital operational resilience they need to comply with, in particular for institutions that hold several authorisations and operate in different markets within the EU. In addition, the double requirements on reporting would be eliminated, thus reducing one of the most significant burdens for financial institutions. This option therefore creates only limited additional administrative and compliance costs for financial institutions and supervisors (especially when compared to the potential costs of cyber incidents), while reducing administrative burden for all financial institutions and in particular for those operating across borders.

[90] According to the impact assessment accompanying the review of the European Supervisory Authorities, (SWD(2017) 308, there are approx. 21.233 entities operating in the EU financial sector. According to the public consultation, mostly all respondents are currently subject to ICT and security incident reporting requirements that either stem from regulation, supervisory expectations or industry best practices (see point 3.2 of Annex 3). If we assume that around 80% of financial institutions are already subject to such reporting, and that due to proportionality and materiality thresholds, between 25 and 50% of institutions would be subject to new rules, this translates into 1000 and 2000 financial institutions.

[91] According to industry data and Commission's calculation, the recurring costs associated to managing and reporting incidents are around €18.000/year for a big European banks. Taking as reference this figure, and using the same methodology and assumptions as for the one-off costs, we could estimate the recurring costs to be in the range of €18 to €36 million.

In terms of disadvantages, this option may not tackle the issues arising from ICT TPPs to the fullest extent. An oversight framework with potential participation of up to 27 prudential supervisors would require convergence and an ongoing dialogue. Moreover, ICT TPP oversight may not eliminate concentration risks given that the ICT TTPs market is currently dominated by four large players, all of them non-European. Indeed, some respondents to the public consultation point out that requirements to limit the concentration of ICT TPPs would be challenging to implement both for financial institutions and for overseers (for more details see point 3.7 of Annex 3).

Effectiveness, efficiency, coherence

Overall, option 2 is effective in achieving the objectives of the initiative at reasonable costs. It also appropriately balances the interaction with the current horizontal EU framework (e.g. the NIS Directive). A comprehensive, coherent and integrated framework for digital operational resilience would enhance the digital dimension of the Single Rulebook compared to the status quo. It would also bring clarity to financial institutions on these aspects, something that the majority of stakeholders responding to the public consultations calls for. This option also minimizes disruption, as some of the measures envisaged are already reflected in general or more specific EU financial provisions.

Impact on stakeholders

Based on the above assessment, the following table summarizes the benefits and costs of the option for each category of stakeholders, while the vertical arrows present the estimated impact for these stakeholders:

	Consumers/investors	Financial institutions	ICT TPPs	Supervisors
Benefits	↑↑↑	↑↑↑	↑↑	↑↑↑
Costs	↑	↑↑	↑↑	↑↑

4.4. Option 3: A financial services digital operational resilience act together with centralised supervision of activities of critical ICT TPPs

Under this option, the Commission would propose a bespoke and detailed EU regulatory framework that would completely replace all existing relevant provisions on ICT risk management across all EU financial services legislation, i.e. repeal all digital operational resilience provisions in level 1 legislation (directives and regulations), and replace all empowerments on the basis of which level 2 legislation (regulatory and implementing technical standards), have been adopted so far. Moreover, to ensure full legal clarity and eliminate residual confusions stemming from overlaps and leading to duplications, the Commission would propose to extract from the NIS Directive the three financial subsectors currently under scope, both from the substantial provisions (incident reporting and ICT requirements), as well as from those related to the NIS "ecosystem" (e.g. CERTs, NIS cooperation group). Cooperation and exchanges of information between financial supervisors and NIS authorities and ENISA would be maintained with the aim that financial supervisors be aware of cyber incidents affecting the economy sectors covered by the NIS Directive. A new Authority for cybersecurity in the financial services sectors would be created to supervise the digital operational resilience related activities of critical ICT TPPs providing their services to financial institutions.

In practical terms, for each of the building blocks this option would entail:

a) **ICT risk management**: full harmonisation in the same way as under option 2.

b) **Incident reporting and information sharing**: again, EU harmonisation regarding incident reporting would be achieved similarly to option 2. However, opposed to option 2, information sharing on key lessons and main vulnerabilities would be not only encouraged, but actually mandated. The Commission would invite competent authorities to create platforms where threat information is shared among peers in a trusted environment and with the participation of relevant competent authorities in their oversight, data analytics or law enforcement capacities.

c) **Digital operational resilience testing**: different from option 2 that is based on mutual recognition of testing results among national authorities, under this option the ESAs would coordinate a European testing exercise. The consequent update for financial institutions based on the testing results would have a prudential impact, too, e.g. on the capital of the financial institution.

d) **ICT third party risk**: going beyond the oversight framework detailed under option 2, the Commission would propose the creation of a new EU authority in the financial sector that would be in charge of *supervising* the activities of critical ICT TPPs when they provide their services to financial institutions. Such authority would closely cooperate with national competent authorities, the ESAs, ENISA, and the ECB. It would be within its mandate to tackle concentration risk by imposing a CRR-inspired large exposure regime on financial institutions, in addition to a registration requirement for all ICT TPPs. In the future, such authority could be integrated under a possible EU cross-sectoral authority supervising critical ICT TTPs that provide services to all EU-based companies.

4.4.1. Assessment of the impact

Benefits

Reduce the risk to financial sector stability and integrity: two out of six specific objectives in Table 2 would be achieved in the same manner as under option 2 (*address ICT security risks more comprehensively* and *testing*). The other four specific objectives would be surpassed.

In terms of novelty compared to option 2, the obligation of financial institutions to report incidents exclusively to the financial supervisor would be made even clearer as a result of disapplying NIS to the financial sector. Currently, and despite the *lex specialis* clause in the NIS Directive, several Member States require multiple and different notifications, sometimes the first notification being processed by the NIS authority, which can be different from the financial supervisor (for more details see point 3.6 of Annex 3). Option 2 would already improve the effectiveness and efficiency of the notification system, as incident notifications would be processed in principle directly by financial supervisors. However, under Option 2 some uncertainty and potential for overlap for financial institutions might remain due to the continued link to the NIS ecosystem, but Option 3 would eliminate that.

Under this option, a coordinated European testing exercise would ensure even more consistent quality and coherent results of digital operational resilience testing across the EU. In addition, under this option a mandatory approach on sharing threat intelligence between financial institutions would be followed. If made mandatory, sharing of information would be less effective as the quality of the information shared would drastically decrease. That is because sharing platforms today have been built over time upon trust, reciprocity and mutual benefit.

A new dedicated Authority would ensure a fully effective supervision of ICT TPPs providing services to the financial sector. While an overwhelming majority of respondents to the public consultation supported the introduction of an oversight framework for critical ICT TPPs, few respondents suggested that a European organization should be responsible with sufficient mandate and authority to perform this task as mostly large, global service providers are in scope. An extension of the remit of existing authorities such as ENISA or BEREC, or a new focused Authority, was also proposed to be used (for more details, see point 3.4 of Annex 3).

Reducing administrative burden and increase supervisory effectiveness: both specific objectives detailed in Table 2 would be achieved under this option.

Costs (direct, indirect, regulatory charges, administrative costs)

For financial institutions: the costs for ICT and testing would be the same as under option 2, with the novelty that 1) administrative burden and uncertainty around incident notification would be reduced even more and 2) significant higher costs would arise because of the *obligation* to share threat intelligence under this option. As mentioned under option 2, the recurring cost estimates for participating in such initiatives range between €1.000 and €50.000, plus 1 to 3 FTEs. Such added costs might not be immediately amortised against the possible losses caused by ICT-related incidents and gains by having access to the right information and the right time.

For supervisors: the costs of ICT supervision would be in line with those under option 2. Costs of supervision of ICT TPPs would be the highest given the set-up of a new Authority, where most staff would be detached from the national competent authorities, at least in the early years after creation. In terms of quantifying the costs associated to setting up a new authority, a benchmark could be used to estimate such costs. Based on previous assessments for supervising comparable operators at EU level,[92] we would estimate the costs associated to new supervisory powers at (i) €5.5 million of one-off costs, and (ii) around 22 FTEs for one authority. Therefore, the total cost covering all three ESAs could be estimated around €16.5 million and around 66 FTEs.

4.4.2. Overall assessment of the option

The main advantage is that this option would provide for a coherent harmonised framework for the financial sector covering all the building blocks and a powerful financial supervision of ICT TPPs. Completely dis-applying the NIS Directive to the financial sector would eliminate any risk of confusion and practical difficulties in the interaction between horizontal and sectoral framework (for example for those cross-border financial institutions that have been designated as OESs in one Member State, but not in the other Member States where they operate, as it would be clear to which authorities they must report). It would also ensure in the

[92] Impact Assessment accompanying the review of the European Supervisory Authorities, (SWD(2017) 308.

best possible way that financial supervisors can combine information from within the financial sector stemming from all Member States and all parts of the financial sector. A direct supervision of ICT TPPs by financial supervisors would ensure that they are in full control of any risks for financial stability and market integrity arising from them.

However, this option would raise several issues:

1) First, the benefit of creating a dedicated authority for ICT third party supervision in the *financial sector*, having a mono-sectoral approach in a landscape where ICT TPPs provide their services cross-sector would be questionable and legally challenging. This could also lead to higher costs and administrative burden for ICT TPPs, which would need to adapt to a multiplicity of different supervisory regimes in all the different sectors to which they provide services (e.g. health, energy, telecoms, etc.).

2) Second, completely dis-applying the NIS Directive to the financial sector could create a gap in the national cyber security strategy of each Member State, and financial supervisors might not be aware of cyber incidents affecting other societal sectors covered by the NIS Directive. This is substantiated by some replies to the public consultation, that stress that being within the NIS universe is good for financial institutions, as they can learn from experiences in other sectors (for more details see point 3.6 of Annex 3). Financial institutions previously covered by the NIS Directive might probably still encounter *practical* difficulties to exit the NIS ecosystem and structures in the context of the review of the NIS Directive.

3) Lastly, even the high level of ambition for digital operational resilience in the financial sector represented by this option could not guarantee the new act to be future proof as ICT risks continuously evolve. Some technicalities around testing would be difficult to solve, such as the risk of concentration of expertise of external testers and the ESAs coordination role in TLPTs. Even with registration requirements for all ICT TPPs, the sub-outsourcing chain could still allow shadow ICT providers located outside the EU to escape supervision by EU financial supervisors.

Effectiveness, efficiency, coherence

Overall, this option would be effective in achieving all the objectives of the initiative, but in a much less efficient way, as the corresponding costs would be significantly higher (e.g. the costs associated with setting up a new authority, to compulsory sharing of threat intelligence, and costs related to the coordination role of the ESAs on the cross-authority testing). In addition, this option would be less coherent with the current horizontal EU framework, as the financial sector would be completely extracted from the application of the NIS Directive, albeit the cooperation and exchanges of information maintained. This could neutralise the benefits resulting from the current cross-authority cooperation established under the NIS Cooperation Group. Therefore, whereas the option would guarantee effectiveness in achieving the objectives, it would do so at high costs and greater incoherence with the current horizontal EU framework.

Impact on stakeholders

Based on the above assessment, the following table summarizes the benefits and costs of the option for each category of stakeholders, while the vertical arrows present the estimated impact for these stakeholders.

	Consumers/investors	Financial institutions	ICT TPPs	Supervisors
Benefits	↑↑↑	↑↑↑	↑	↑↑↑
Costs	↑	↑↑	↑↑↑	↑↑↑

4.5. Comparison of options

Table 4 below summarises the extent to which the options are effective, efficient and coherent. The effectiveness of the options is mapped against the specific objectives set out in section 3. The respective scores are attributed based on the detailed analysis performed under each of the options. The scores represent the sum of pluses and minuses.

Table 4 – Summary of options in terms of effectiveness, efficiency and coherence

	Effectiveness			**Efficiency**	**Coherence**	**Score**
	Objective 1: Reduce the risk of financial disruption and instability	Objective 2: Reduce administrative burden	Objective 3: Increase consumer and investor protection			
"Do nothing"	0	0	0	0	0	0
Option 1	–	–	+	+	++	2
Option 2	++	++	++	+	+	8
Option 3	++	++	++	≈	≈	6

Magnitude of impact as compared with the "do nothing" scenario (the "do nothing" scenario is indicated as 0): ++ strongly positive (score 2); + positive (score 1); – – strongly negative (score -2); – negative (score -1); ≈ neutral (score 0);

Table 4 shows that option 1 is not effective in terms of meeting the objectives, whereas options 2 and 3 are very effective. Option 1 would not reduce administrative burden (objective 2) given the higher capital needed to create the new buffers, hence a "-". Capital buffers do not reduce ICT risks (objective 1), hence a "-". Only post incidents can they help financial institutions overcome the losses incurred, but they would not contribute to building up institutions' operational resilience (e.g. preparedness and ability to withstand and recover). Capital buffers would still be an efficient way forward because better-capitalised institutions could better withstand the losses caused by ICT disruptions, and also reduce the potential impact on their customers, hence a "+".

The main difference between options 2 and 3 is their efficiency, as option 3 is more costly to implement, and their coherence. In option 3, the higher costs for setting up a new authority and mandatory participation in information sharing platforms would be compensated by the ESAs coordination of testing exercises and the complete extraction from NIS, that would do away with all duplications on incident reporting that might still subside if the financial sector stayed associated with NIS, hence a neutral score "≈". In terms of effectiveness, both option 2 and 3 reduce risks to financial stability and reduce administrative burdens.

In terms of coherence, option 1 scores the best, while option 3 is the least coherent with the current horizontal EU framework due to the complete extraction from NIS. In sum, the option which promises the best possible balance across the three criteria of effectiveness, efficiency and coherence is option 2.

After having established how the options score in terms of effectiveness, efficiency and coherence, table 5 below presents how the options score in terms of the level of stakeholder support.

Table 5 – Summary of pros/cons and stakeholders support

Options	Total score for Effectiveness/ efficiency/ coherence	Stakeholders support
Option 1	Low (2)	*Low*
Option 2	High (8)	*High*
Option 3	Medium (6)	*Medium*

Table 5 shows that options 2 presents the best combination of the criteria of effectiveness, efficiency and coherence underlined by the high score. At the same time, stakeholders support is high for option 2, medium for option 3, while it is low for option 1[93].

4.6. Retained option

In light of the above comparison, the retained option is **Option 2: a digital operational resilience act for the financial sector**. 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. Under this option, a comprehensive digital operational resilience act for the EU financial sector would bring a coherent and integrated framework for digital operational resilience and would enhance the digital dimension of the Single Rulebook. At the same time, this option minimises disruption and transition costs with respect to the existing EU financial services legislation. It furthermore appropriately balances the interaction with the current horizontal framework (e.g. the NIS Directive), and accommodates the different features of the initiative with the consistency that is necessary for achieving coherence at EU level.

Option 1 which would imply an increase in capital requirements for financial institutions is not considered feasible to implement, less so in an economic recession context. Indeed, in the context of COVID-19, several Member States and the ECB have taken additional measures to alleviate the expected adverse effects of the outbreak on the economy. At international level, the BCBS has also decided to delay the implementation of the new Basel rules to strengthen the capital of banks. Similarly, Option 3 would entail substantial costs for setting up a new dedicated agency for the oversight of TPPs, and therefore this option is also not considered viable in the current context.

In Annex 4, the detailed provisions under the retained option are described, giving an indication of what possible core requirements might entail in practice.

[93] Even though the public consultation did not include questions on quantitative measures such as capital charges, several respondents provided feedback on this issue. Overall, they highlighted that developing rules requiring financial firms to hold sufficient capital may serve as proxies for increased trust in the financial sector, but will have limited effectiveness in tacking cyber risks. In addition, it will drive firms' resources to satisfy regulatory compliance, rather than continuously assessing their maturity and posture to build increased levels of resiliency.

5. OTHER SPECIFIC IMPACTS OF THE RETAINED POLICY OPTION

5.1. Impacts on SMEs

The policy option chosen would have several positive effects on SMEs operating in the financial services industry. Direct benefits stem from the fact that the retained option will define a clear and standardised digital operational resilience framework across the EU financial sector. Furthermore, the proportionality enshrined in the option (for example limiting advanced testing to the most systemic financial institutions) ensures that higher digital operational resilience does not come with disproportionate economic costs. Proportionality will be designed in terms of scope and intensity, through the use of qualitative and quantitative assessment criteria to ensure that while the new rules cover all financial entities, they remain in the same time tailored to risks and needs of specific entities as well as to their size and business profiles.

By strengthening the digital security and resilience components of the EU Single Rulebook, market participants will benefit from a single set of rules for sound and proper digital operational risk management, for incident notification (in particular by limiting duplications of reporting requirements) and testing. Furthermore, a harmonised set of rules would allow SMEs to take up European and international standards that can have a positive impact on their capacity to operate cross-border.

Finally, the new EU regulatory framework will bring clarity to SMEs on the different rules on digital operational resilience they need to comply with, in particular for institutions that hold several authorisations and operate in different markets within the EU. This would be of a particular added value for smaller and medium sized financial institutions that in general have less resources for hiring consultancy and legal advice firms for assessing them on compliance with the complex regulatory framework.

5.2. Social impacts

The main social impacts of the retained policy option would be on consumers and investors. Digital operational failures and incidents may trigger severe direct and indirect consequences for the EU financial system and its participants.

Through the creation of a standardised set of rules governing digital operational resilience in the financial sector, market participants will be encouraged to invest in technological solutions to ensure higher levels of security, thus enhancing the ecosystem's overall resilience. It is reasonable to expect that to higher levels of digital security of the EU financial system corresponds a decrease in the number of incidents, in their average cost as well as in less reputational consequences for affected entities. Hence, as also highlighted by the majority of the responses to the public consultation, the entire ecosystem will be perceived as safer and more resilient, especially by end-users, once the retained policy option will be applicable. The society as a whole would benefit from the increased trust in the financial services industry.

Again, given that COVID-19 may further accentuate the digitalisation of financial services, the benefits associated with measures ensuring digital operational resilience are likely to increase.

5.3. Environmental impacts

In the EU, energy consumption in the services sector increased annually by 0.6% on average in the period 2005-2017.[94] The energy demand of electrical appliances, in particular of ICT appliances and other energy-intensive technologies, is increasing. It is therefore important to encourage the adoption of low-emission technologies[95] in line with the objectives set out in the Commission Communication on the *European Green Deal* and the Commission *Industrial Strategy*.[96]

The policy option chosen would encourage an enhanced use of the latest generation ICT infrastructures and services, which are environmentally more sustainable. It will also provide legal clarity on the arrangements with ICT TPP, which in turn is expected to increase their use. ICT TPPs are in general more energy efficient than in house ICT infrastructure. The higher efficiency levels of recent security technologies and infrastructures will contribute to a reduction in the consumption of electricity, of water and other liquids used to cool data centres, thus having a positive impact on the environment through the reduction of harmful emissions. New and smart technologies also are built with eco-friendly materials, which will facilitate the recycling after their lifecycle is completed.

6. MONITORING AND EVALUATION

This section describes the measures to monitor and evaluate the impact of the preferred option on the specific objectives.

The first review will 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 evaluation accompanied where appropriate by a proposal for its review. The review could be supported by a public consultation, studies, expert discussions, surveys, workshops, etc.

Table 6 provides a list of indicators that will be used to monitor progress towards achieving the objectives.

Table 6 - List of indicators to monitor progress towards achieving the objectives

Objectives	Monitoring indicators	Sources of data
General Objective 1: Reduce the risk of financial instability		
• **Specific objective 1**: address ICT security risks more comprehensively and strengthen the overall level of digital resilience of the financial sector	1) Number of ICT-related incidents in the EU financial sector and their impact	ESAs
• **Specific objective 2**: enable financial supervisors' access to information on ICT-related incidents	2) Number of significant ICT security incidents reported to prudential supervisors	ESAs
• **Specific objective 3**: ensure that financial institutions assess the effectiveness of their preventive and resilience capabilities and	3) Number of financial institutions that perform a TLPT tests	ESAs Industry feedback

[94] https://www.eea.europa.eu/data-and-maps/indicators/final-energy-consumption-by-sector-10/assessment.
[95] https://ec.europa.eu/info/sites/info/files/european-green-deal-communication_en.pdf.
[96] https://ec.europa.eu/commission/presscorner/detail/en/fs_20_425.

identify ICT vulnerabilities		
• **Specific objective 4:** strengthen the outsourcing rules governing the indirect oversight of ICT TPPs	4) Number of financial institutions using Standard Contractual Clauses	ESAs Industry feedback
• **Specific objective 5:** enable a direct oversight of the activities of ICT TPPs	5) Number of ICT TPPs overseen by prudential supervisors	ESAs
• **Specific objective 6**: incentivise the exchange of threat intelligence in the financial sector	6) Number of financial institutions participating in TI solutions	ESAs Industry feedback
General Objective 2: Reduce administrative burden		
• **Specific objective 1**: streamline ICT-related incident reporting and address overlapping requirements	7) Number of authorities to report the same incident	ESAs Industry feedback
• **Specific objective 2**: reduce single market fragmentation and enable cross-border acceptance of testing results	8) Number of cross-border TLPTs	ESAs Industry feedback

In terms of the reporting and collecting the data, indicators 1, 2 and 5 would be provided by the ESAs. Indicators 3, 4, 7 and 8 are to be provided by both supervisors and financial institutions. Finally, concerning indicator 6, given the voluntary nature of the measures envisaged, this indicator will need the involvement of the industry.

The ESAs will collect the data on these indicators on an annual basis. In addition, at the beginning of each year the ESAs should (where applicable) set targets vis-à-vis the indicators to allow comparison to the previous year.

ANNEX 1 – PROCEDURAL INFORMATION

1. Lead DG, Decide planning / CWP references

This Impact Assessment Report was prepared by Directorate B "Horizontal policies" of the Directorate General "Directorate-General for Financial Stability, Financial Services and Capital Markets Union" (DG FISMA).

The Decide Planning reference of the "Digital Operational Resilience of Financial Services (DORFS) Act" is PLAN/2019/6126.

The initiative on strengthening the digital operational resilience of the EU financial sector entities was included in the 2020 Commission Work Programme published on 29.01.2020.

2. Organisation and timing

Three Inter-Service Steering Group (ISSG) meetings were held in 2020. The ISSG consisted of representatives from various Directorates-General of the Commission: CNECT, HOME, COMP, GROW, JUST, TAXUD, ECFIN, RTD, DEVCO, NEAR, JRC, and SJ. The ISSG met on 4 March 2020, 2 April 2020 and 22 April 2020. The meetings were chaired by SG.

The contributions of the members of the Steering Group have been taken into account in the content and shape of this impact assessment.

3. Consultation of the Regulatory Scrutiny Board (RSB)

The Impact Assessment report was examined by the Regulatory Scrutiny Board (RSB) on 27 May 2020. The RSB gave a positive opinion with reservations on 29 May 2020.

DG FISMA has updated the impact assessment report to incorporate the recommendations received by the Regulatory Scrutiny Board.

Main considerations	
RSB recommendation	**Response to RSB's recommendation**
1) The report does not sufficiently focus on the political decisions to take. It does not provide enough information to judge issues of proportionality.	The impact assessment has been revised to more clearly explain how proportionality would be embedded in the initiative.
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.	The impact assessment has been revised to further explain the extent to which the initiative takes into account the joint technical advice from the European Supervisory Authorities, as well as international guidance and best practices.
3) The report does not demonstrate that the preferred option is the optimal solution.	The impact assessment has been revised to further substantiate the comparison of the different options.
4) The report does not adequately explain how this initiative would work together with parallel EU legislation that is also under	The impact assessment has been revised to further explain the interaction with the existing horizontal legislation (e.g. NIS Directive and ECI Directive).

revision.	

4. Evidence, sources and quality

The impact assessment has been carried out with the comprehensive qualitative and quantitative evidence from various recognised sources, including the two joint technical advices by the European Supervisory Authorities (ESAs). The source of the analysis also included a targeted public consultation with stakeholders, which ran from 19 December 2019 until 19 March 2020.

The quality of the publicly available reports and research can be considered high as they represent the best available information from the supervisory authorities (e.g. reports by ESRB, ECB, BCBS, FSB, G7, IMF, etc.) and leading industry research, and include quantitative and qualitative input from identified stakeholders across the global financial sector.

The Commission has identified limitations on the available data on incident reporting and on disclosures on expenses/costs associated to cyber security in general by financial institutions and ICT TPPs. On the one hand, figures on incident reporting are not available as this data is not compulsory to disclose by financial institutions, and is only reported to financial supervisors in a limited number of subsectors. On the other hand, there is a general lack of evidence on expenses/costs associated to cyber security, as financial institutions and ICT TPPs are reluctant to disclose and share such information, due to concerns that reporting on these topics could potentially harm them.

ANNEX 2 – OVERVIEW OF THE REGULATORY FRAMEWORK CONCERNING DIGITAL OPERATIONAL RESILIENCE

1. ICT risk management

Financial sector legislation

A short comparison below shows disparity of the ICT risk coverage across the financial sectors.[97] This, together with the responses to the public consultation and a comparison between the status quo and the preferred option of EU intervention detailed in Annex 4 (Table 8 - Overview of main changes to the building blocks between the "do nothing" scenario and preferred option), support the conclusion that the effectiveness, efficiency, coherence, relevance and EU added value of the current ICT risk provisions have been rather limited.

In the **banking services** area, the applicable legislation (CRD IV) sets out internal governance rules and general operational risk provisions that serve implicitly as a basis for ICT risk management measures. Additionally, the EBA Guidelines on ICT risk management security risks,[98] the application of which starts on 30 June 2020, will set non-binding expectations in relation to the way credit institutions, investment firms and payment service providers should manage their internal and external ICT risks. In the COVID-19 context, the Guidelines implicitly cover the need for cybersecurity within a financial institution's information security measures and aim to ensure a consistent and robust approach across the single market. The **payment services** component, through its dedicated framework (PSD2) goes beyond the CRD IV baseline. It contains bespoke rules already at the authorisation stage[99] (ICT security controls and mitigation elements), security-related provisions throughout the ongoing management of operational and security risk (implicitly referring to ICT risk),[100] but developed further at the level of EBA guidelines[101] to include specific provisions on the ICT incident reporting - explained later in section 2- and separate rules on strong customer authentication.[102]

The current legislation in the **insurance and re-insurance** sector comprises rather general provisions on governance and risk management, thus capturing ICT risk / ICT risk management in an implicit and partial way. Different elements - also relevant for the ICT risk management - (contingency plans, effective risk management systems, processes to identify, measure, monitor, manage, report risks, risk assessment, etc.) may support the ICT risk management cycle functions in the absence of more dedicated provisions. Certain requirements on governance and risk management have been developed in Level 2

[97] This comparison is not meant to be an exhaustive analysis (not every single requirement is mentioned).
[98] EBA Guidelines on the mitigation and management of information and communication technology (ICT) and security risks for banks in EU (EBA/GL/2019/04). They are addressed to the institutions in scope (credit institutions, investment firms and payment services providers) and will complement and be read in conjunction with other sets of guidance, in particular EBA guidelines on ICT risk assessment under the Supervisory Review and Evaluation Process (EBA/GL/2017/05) (which are addressed to the supervisors) and EBA guidelines on outsourcing arrangements (EBA/GL/2019/02).
[99] This is not however a unique feature to PSD. Several other financial sectors contain some requirements for information pertaining to the IT systems to be reported to supervisors at the stage of authorisation.
[100] Article 95 PSD.
[101] EBA Guidelines on security measures for operational and security risks of payments services under the revised Payment Services Directive.
[102] Articles 97-98 PSD and related COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

legislation[103] with or without specific references to ICT risk. Furthermore, as the current guidelines on governance set at EU level have insufficiently addressed ICT risk / ICT security, Members States started defining national rules which, although comparable, do not always fully converge. To address the fragmentation and lack of more dedicated provisions, EIOPA is consulting on Guidelines on ICT security and governance,[104] When it comes to **institutions for occupational retirement** (IORPs), the applicable legislation[105] is even less specific on the ICT risk / ICT security components, which essentially remain (implicitly) subsumed to generally worded provisions on risk management and governance.

The situation in the securities market is rather uneven**.** At the high end of the range, **central securities depositories** (CSDR) and central counterparts (EMIR) are subject to more specific rules on ICT risk. CSDR explicitly acknowledges that operational risk applies to deficiencies in information systems, and EMIR sets out some ICT risk/ICT security tailored provisions. Within its operational risk architecture, CSDR requires central securities depositories to have appropriate IT tools, controls and procedures ensuring a high degree of security and operational reliability, while a Commission delegated act further specifies some components in the ICT risk management cycle. By way of example, that delegated act[106] requires central securities depositories to have comprehensive frameworks for the information security and the management of risk (including incorporation of new technological developments), adapted policies and procedures to identify risks, to integrate the operational risk management system into the daily risk management process, to establish procedures to record, monitor and resolve operational incidents, to identify potential single points of failures and address risks posed by all categories of market players. Separate requirements are devoted to the IT tools and systems (required to be resilient, possess sufficient capacity, attain service level objectives, rely on internationally recognised technical standards and be subject to stringent IT testing) and to the elements of the information security framework. The post-incident stages are addressed through dedicated provisions on business continuity policy and disaster recovery, while certain governance-related elements are also present in the different stages (i.e. requirement to have an operational risk management function; the explicit role of the management body in the management risk framework/business continuity policy/associated recover plan; the establishment of chief risk officer and chief technology officer functions with direct access to the management body).

In a relatively comparable manner (even though less detailed), EMIR echoes for **central counterparties** certain requirements for the IT systems, such as to adequately deal with the complexity, variety and type of services, to ensure a high degree of security, integrity and confidentiality of the information. A set of articles are devoted to the post-incident stage. EMIR Delegated Regulation[107] sets out more granular requirements for the risk management and internal control mechanisms, IT systems, record-keeping process, while also tackling

[103] COMMISSION DELEGATED REGULATION (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).
[104] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-information-and-communication-technology-security-and-governance_en.
[105] Directive (EU) 2016/2341 on the activities and supervision of institutions for occupational retirement provisions.
[106] COMMISSION DELEGATED REGULATION (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories.
[107] COMMISSION DELEGATED REGULATION (EU) No 153/2013 of 19 December 2012 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on requirements for central counterparties.

components of business continuity, business impact analysis, disaster recovery, crisis management and communication.

Investment firms and trading venues stand somewhere in the middle of the range. **Investment firms** are covered by general organisational requirements addressing the need for effective arrangements for information processing systems, sound security mechanisms to guarantee the security and authentication of the means of transfer of information, minimise the risks of data corruption and of unauthorised access and prevent information leakage (MIFID).[108] These requirements are further specified in a Commission Delegated Regulation[109] addressing procedures and systems that safeguard the security, integrity and confidentiality of data, as well as the business continuity and recovery needs.

More stringent or detailed rules[110] apply to **investment firms performing algorithmic trading**, in particular to have effective systems and risk controls to ensure the resilience of trading systems, prevent erroneous orders or misuse of such trading systems; to have business continuity arrangements enabling them to deal with the failure of trading systems and to undergo full testing and monitoring of such systems. In the same vein, *trading venues* allowing or enabling algorithmic trading are subject to more thorough rules[111] covering their systems' resilience and capacity (including under severe market stress), calling for an appropriate testing of algorithms, for business continuity arrangements to address disruptive incidents (including a requirement to resume trading within or close to two hours from the incident and ensuring that the maximum amount of data that may be lost from any IT service of the trading venue after an incident is close to zero), setting out the minimum content for business continuity plans and requiring a periodic review of such plans, in addition to security and limits to access provisions and certain governance related rules.

At the lower end of the range, less comprehensive or less specific provisions apply to trade repositories, data reporting service providers, credit rating agencies and asset management companies. **Trade repositories** are subject to general operational reliability requirements that include secure and reliable systems with adequate capacity to handle the information received, general requirements to implement business continuity policies and disaster recovery plans, safeguarding data, recordkeeping policy and data availability mechanisms.[112]

Obligations for **data reporting service providers** include sound security mechanisms (to guarantee the security of the means of transfer of information, minimise the risk of data corruption and unauthorised access and prevent leakage) while few more specific

[108] DIRECTIVE 2014/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.
[109] COMMISSION DELEGATED REGULATION (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.
[110] COMMISSION DELEGATED REGULATION (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment firms engaged in algorithmic trading.
[111] MIFID and COMMISSION DELEGATED REGULATION (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venues.
[112] EMIR and COMMISSION DELEGATED REGULATION (EU) No 150/2013 of 19 December 2012 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories with regard to regulatory technical standards specifying the details of the application for registration as a trade repository

requirements for electronic security derive from Level 2,[113] including the set-up of procedures and arrangements to protect IT systems from misuse / unauthorised access, minimise risks against information systems, prevent unauthorised disclosure, and to ensure the security and integrity of data.

Credit rating agencies are required to have effective control and safeguard arrangements for the information processing systems and employ appropriate systems resources and procedures to ensure the regularity and continuity in the performance of credit rating activities. Level 2 legislation[114] requires record keeping and business continuity planning, with a separate article dedicated to the information processing systems (description of such system and back-ups, description of control and safeguard arrangements for information processing systems, identity of the senior manager responsible for these systems).

In the area of **collective asset management**, UCITS and AIFMD contain few provisions specifically dedicated to ICT risk/ICT security. Some explicit provisions on effective control and safeguard arrangements for information processing systems are present in UCITS. UCITS's Implementing Directive [115] and AIFMD's Delegated Regulation[116] - also building on more general provisions for risk management and principles such as due skill, care and diligence - specify a set of requirements relevant to the ICT risk - notably references to adequate systems/procedures to safeguard the security, integrity and confidentiality of information; to have adequate business continuity policy to ensure - in case of interruption - the preservation of essential data and functions and the maintenance of services or the timely recovery of data and functions and timely resumption of services; appropriate arrangements for suitable electronic systems to permit a timely and proper recording of portfolio transaction or subscription or redemption orders, as well as requiring a high level of security during the electronic data processing, the integrity and confidentiality of the recorded information. In addition, some more general provisions on risk management policy, measurement and management of risks, or qualitative requirement also apply.

Even less specific provisions apply to **statutory auditors and audit firms**, the relevant EU legislation[117] containing general provisions on internal organisation with some limited references to effective control and safeguard arrangements for information processing systems, as well as the use of appropriate systems, resources and procedures to ensure continuity and regularity.

Effectiveness, Efficiency, Relevance, Coherence, EU-added value

[113] COMMISSION DELEGATED REGULATION (EU) 2017/571 of 2 June 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards on the authorisation, organisational requirements and the publication of transactions for data reporting services providers.
[114] COMMISSION DELEGATED REGULATION (EU) No 449/2012 of 21 March 2012 supplementing Regulation (EC) No 1060/2009 of the European Parliament and of the Council with regard to regulatory technical standards on information for registration and certification of credit rating agencies.
[115] COMMISSION DIRECTIVE 2010/43/EU of 1 July 2010 implementing Directive 2009/65/EC of the European Parliament and of the Council as regards organisational requirements, conflicts of interest, conduct of business, risk management and content of the agreement between a depositary and a management company.
[116] COMMISSION DELEGATED REGULATION (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision.
[117] Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC.

Effectiveness analysis considers how successful EU action has been in achieving or progressing towards its objectives. None of the pieces of financial services legislation detailed above had at its objectives operational resilience and digitalisation, not even operational risk with its sub-component ICT risk. EU action greatly delivered on its objectives to ensure financial stability, a single set of harmonised prudential rules which financial institutions throughout the EU must respect. Those targets have largely been achieved. Therefore, an effectiveness analysis is difficult to carry out when factors driving progress did not include preparing for, monitoring and dealing with operational incidents and disruptions.

Efficiency focuses on the relationship between the resources used by an EU intervention and the effects and changes generated by intervention. With the aim to reduce inefficiencies -particularly unnecessary regulatory costs-, and simplify the intervention, the financial services legislation has conceptually moved from minimum harmonisation to maximum harmonisation and from regulating via directives to regulations. A collective analysis of administrative and regulatory burdens is again difficult to carry out in the context of EU initiative covering around 12 financial subsectors.

Relevance looks at the relationship between the needs and problems identified and the objectives of the EU intervention. Consideration must be given to whether the objectives of an EU intervention correspond to wider EU policy goals and priorities. All the enumerated EU interventions helped to address needs and problems that were present in the aftermath of the 2008 financial crisis: banks were not sufficiently capitalised, financial markets were not sufficiently integrated, and harmonisation up until that point had been kept minimal. ICT risk was not considered a priority then, and as a result the legal landscape for the different financial subsectors has evolved in an uncoordinated manner.

The evaluation of **coherence** involves looking at how well or not different actions work together. The rules on operational resilience -where available- are patchy, uncoordinated and do not respond to the increased risk of operational disruptions that financial institutions, no matter the subsector they are active in, or their size and importance, face nowadays especially due to the interconnectedness of the financial sector as a whole. The approaches taken so far have led to inefficiencies and a lack of coordination and complementarity to address ICT risks, where, in the absence of EU rules (or too basic EU requirements), international bodies, Member States or supervisors have filled in the gap.

The **EU-added value** is the creation of financial stability and the deep level of integration of the financial sector nowadays, which could not have been achieved with or expected from national actions by the Member States: the SSM, the ESAs, the Single Rulebook. However, when it comes to ICT risk management requirements on ICT risk, the lower and higher end of the spectrum show that some measures have had limited impact, while others have provided more EU harmonisation.

The responses to the public consultation show extended support to enhance the ICT risk management framework for all financial institutions. Most respondents insist that these common standards should be principle and risk based and allow for a proportionate application. In the absence of more EU harmonisation, many financial institutions have voluntarily established and implemented security measures to manage and mitigate ICT risks, following national rules, EU soft rules (e.g. EBA guidelines) or global standards (e.g. ISO).

The NIS Directive

Adding to the intricacy inside the financial sector, further complexity emerged from the interplay with a horizontal legal framework in relation to the security of network and information, namely the NIS Directive. NIS is the first EU-wide legislation passed in the area of cybersecurity. It is a directive with a larger remit, applying to six distinct areas, ranging from energy (electricity/oil/gas), transport (air, rail, water and road), financial services (see below) to health (health care settings, including hospitals and private clinics), drinking water supply and distribution and 'digital infrastructures'. In finance, only banking (credit institutions) and FMIs areas (operators of trading venues and central counterparties) are covered.

The design of the NIS Directive revolves around the identification of operators of essential services (OESs) in these sectors and the imposition of "state of the art" requirements on security and incident notification. One problem derives from the focus on OESs. The process of identification of OESs relies on (general) criteria defined at EU level by the Directive, but at the same time a wide discretion is given to the Member States as regards the final outcome of this process. In practice, although the three financial sectors are subject to the NIS Directive, not all financial institutions active in these sectors have been designated as OES and are thus now covered by the transposition of the NIS Directive into national frameworks. Moreover, this designation varies across the Union, leading to uneven implementation. This approach is suboptimal for the needs of an ecosystem as integrated as finance, which prerequisites a common baseline for its digital operational resilience and is already subject to a Single Rulebook and supervisory convergence. Secondly, the current NIS Directive requirements on security and incident notification are general, while the financial sector needs more granularity to cover not only those aspects of operational resilience, but also aspects not explicitly covered by NIS (testing and third party dependencies). Thirdly, the NIS Directive provides for a *lex specialis* clause, prescribing that sector specific legislation that contains at least equivalent security and incident notification requirements applies instead of the NIS Directive. The Commission further clarified the application of this clause.[118] However, as shown above, since sector-specific legislation in finance has not always captured, properly or explicitly, ICT risks, some inadvertent overlaps and/or difficulties in the interpretation of this interplay surfaced. Moreover, some Member States have gone even further in the implementation of the NIS Directive and enlarged the scope of national transposition laws to also cover other financial sectors (i.e. insurance).

2. Incident notification

The NIS Directive requires major incident reporting for certain banks, trading venues and CCPs identified as OES, when the incident has a significant impact on the continuity of the OES's services: the process involves the designated NIS authority and notifications must be sent without undue delay.

Requirements in financial legislation to report major operational incidents to financial supervisors have been quite limited: PSD2 (with its subsequent EBA Guidelines on major incidents reporting under PSD2)[119] is deemed more detailed and stringent than the NIS

[118] Section 5 of the Communication. For instance PSD2 is *lex specialis* for both security requirements and incident notification and MIFID and EMIR are *lex specialis* for security requirements, thus taking precedence over the relevant requirements of the NIS Directive.

[119] EBA Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2), EBA/GL/2017/10, https://eba.europa.eu/sites/default/documents/files/documents/10180/1914076/3902c3db-c86d-40b7-b875-dd50eec87657/Guidelines%20on%20incident%20reporting%20under%20PSD2%20(EBA-GL-2017-10).pdf.

incident reporting and thus takes precedence. Major incidents experienced by **payment service providers** must be notified to the national competent authorities, EBA and ECB within 4 hours from the moment of detection. **Operators of trading venues**, as well as **investment firms** engaged in algorithmic trading and **data reporting service providers** are required by Level 2 provisions to promptly inform their competent authority of any successful breaches in their physical and electronic security measures. The general nature of the requirements applicable to trading venues means that they cannot be deemed *lex specialis* in relation to the NIS incident reporting obligations. **CSDs** are subject to very general obligations to inform the competent authority on operational incidents and to communicate a post-incident review to the competent authority. **Banks** must report incidents on the basis of NIS only if they have been identified as OES and if the incident has significant impact on the continuity of the bank's services.[120] The other financial institutions are not covered by any incident notification requirements.

There are no EU rules on information sharing between financial institutions.

Effectiveness, Efficiency, Relevance, Coherence, EU-added value

An evaluation of the NIS Directive is not the purpose of this Annex, however its provisions overlap with some of the incident notification rules in the financial services acts mentioned above, and that has led to double reporting and added complexity (differences in taxonomy, reporting timeframes, data to be notified, templates or relevant thresholds triggering the reporting of an incident). Despite the *lex specialis* exemption, banks identified as OES that also hold a payment service provider licence are expected to report the same incident to several authorities and as a consequence incur excessive compliance costs. This translates into a limited **efficiency** and **coherence** of the EU intervention. Trading venues must anyway report to the financial supervisor based on the MiFID requirements and to the NIS authority based on NIS, if identified at national level as OES.

In the public consultation, the big majority of respondents agree that a comprehensive and harmonised EU-wide system of ICT incident reporting should be designed for all financial entities: a uniform scheme, uniform criteria and via a single reporting path.

3. Testing

Only four types of financial institutions are subject to some rules on testing. Requirements to test IT tools, systems and procedures can be found in relation to **payment service providers** and **CSDs**. **CCPs** are required to perform stringent testing, simulating stressed conditions, before initial use, after making significant changes and after a major disruption has occurred. Penetration testing is mandated for **investment firms** engaged in algorithmic trading only.

Effectiveness, Efficiency, Relevance, Coherence, EU-added value

The EU intervention has had very limited **effectiveness** and **EU-added value**, hence the proliferation of national and supervisory sponsored testing frameworks, which, because of their legal nature, could –if and when applied in different Member States- lead to inconsistencies and excessive compliance costs for financial institutions and supervisors alike.

[120] Banks must also report to the SSM if they are significant, but the SSM incident notification scheme is not a regulatory framework, and the scope of this annex is to describe and shortly evaluate EU legal provisions only.

The majority of respondents to the public consultation face issues with overlapping or diverging testing obligations. Especially those financial institutions with locations in multiple Member States are often confronted with overlapping requirements for ICT tests by different authorities, which tie up considerable resources. Therefore, these respondents believe that harmonizing the requirements for ICT tests, reducing compliance complexity by integrating regulatory guidance, expectations and requirements would benefit all private and public market players.

4. Third party risk

The regulatory framework dealing with risks stemming from institutions' reliance on third parties is composed of on *outsourcing* and further sub-outsourcing rules that are again patchy: except statutory auditors and audit firms, all financial institutions must observe either all (MiFID and IORPS) or only some general obligations for all of their outsourcing arrangements:

1) the management bodies and senior management of certain financial institutions (**payment service providers, banks, investment firms, operators of trading venues, CCPs, CSDs, insurance undertakings, data reporting service providers and IORPS**) remain responsible and accountable for the activities and services they perform and provide even when they outsource them or parts thereof to TPPs. This is a key principle underpinning the existing regulatory framework on outsourcing, including the EBA Outsourcing Guidelines[121] and the EBA Guidelines on internal governance.[122]

2) **investment firms, operators of trading venues, CSDs, trade repositories, credit rating agencies and IORPs** must outsource through a written contract; and

3) any outsourcing must be notified to the competent authority (**payment service providers, trading venues, insurance undertakings, asset managers and IORPs**).

For **banks, investment firms, payment institutions and e-money providers**, the EBA Outsourcing Guideline foresee that a third party service provider should grant institutions and competent authorities complete access to premises to and unrestricted rights of inspection and auditing. The same goes for the EBA Recommendations on cloud outsourcing, whereby cloud service providers shall provide competent authorities full access to premises, and unrestricted rights of inspection. Moreover, the EBA Outsourcing Guidelines require to maintain and update a register of all outsourcing arrangements with cloud service providers. Such a register will be available only starting December 2021 and will only cover outsourcing arrangements with a subset of ICT TPPs -cloud service providers-, have a limited coverage of the supply chain and no common templates for data reporting.

Only 3 financial services acts devote special attention to *outsourcing to critical service providers*, especially the CSDR: **CSDs and CCPs** must identify critical service providers and manage dependencies; CSDs and data reporting service providers must inform competent

[121] https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.
[122] https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf.

authorities on dependencies with critical service providers; CSDs must also have robust arrangements for the selection and substitution of IT third party service providers; lastly, **investment firms** must carry out due diligence when outsourcing to TPPs and MIFID includes a specific provision on outsourcing to third party service providers located in a third country.

The EU financial services regulatory landscape contains no provisions on the *oversight* of third parties. The NIS Directive has digital service providers under its scope (cloud service providers being among them), that come under the supervision of the NIS authority for their security and incident reporting obligations under NIS. Therefore, only a limited subset of ICT TPPs are subject to a limited range of supervision that, besides, is carried out by 27 NIS authorities.

Effectiveness, Efficiency, Relevance, Coherence, EU-added value

The existing legal provisions on outsourcing have had an **EU-added value**: bringing in unregulated entities that operate cross-border and come from outside the financial sector and summiting them to an indirect supervision by financial supervisors needed a harmonised EU approach. Such harmonisation could not have been expected from national actions by the Member States. As a result of the **relevance** of the EU intervention, those financial subsectors where there are no such legal provisions have had to come up with level 3 acts (EBA guidelines) to fill in the gap. However, the difficulties financial institutions face when negotiating their written contracts with ICT TPPs are an indicator of poor **efficiency**.

The results of the public consultation highlight that certain EU jurisdictions have more stringent requirements for outsourcing and require certain data localization or pre-approvals from regulators, which may be in conflict with other laws, e.g. the GDPR and the current EU-wide initiatives for the free flow of data. The lack of standardization in controls, processes, and reporting across industry results in unnecessary complexity and frustration for both financial institutions and third parties.

*Table 7 – Mapping of existing (qualitative) provisions on digital operational resilience in the EU financial services L1 and L2 legislation**

Building block	Main elements of the buiding block	EU financial services Level 1 and Level 2 legislation												
		Payments (PSD2)	Banks (CRD/CRR)	Investment firms (MIFID)	Trading Venues (MIFID)	CCPs (EMIR)	CSDs (CSDR)	Trade Repositories (EMIR)	Insurance (Solvency II)	Asset Management (UCITS/AIFMD)	CRAs	Data Reporting Service Providers (DRSPs)	Audit	IORPs
ICT risk management	Arrangmenents (policies, procedures and systems) on risks to which the entity is exposed to		art. 74(1)	art. 16(4), (5)	art. 47 (1)	art. 26(1)	L2 - art.48(1)	Art 79		L2 - art. 40(1) - both art. 15(2) - A	Annex I - Section A, (4)			art. 28(3)
	Operational risk framework / policy	art. 95(1)				Art. 28 (risk committee)	L2 - art. 79(1)			L2 - art. 13(1) - A				
	Risk management policy			L2 - art. 23(1)		L2 art.4			art. 41(3)	L2 - art. 38(1) - U				art. 25(1)
	Information security framework/strategy	art. 95(1)		L1 - art. 18 (AT)		L2 - art. 9(3)	L2 - art. 79(5), art. 75(5)							
	Appropriate IT tools, reliable, resilient and secure systems (to ensure security / integrity / confidentiality)	art. 95(1), art. 97(3) L2 - chapter II,IV,V		art. 16(5) L2 - art. 21(2)	art. 48(1) L2 - art. 23(1),(2)	art. 26(6) and L2 art.9	art. 45(1) L2 - art. 75	L2 - art. 79(1)	L2 - art. 258(1)	L2 - art. 57(3) - A		art. 64 (4), 65(5), 66(3) + L2 - art. 9(1)		
	Business continuity policy		art. 85(2)	art. 17 (1) and L2 - art. 14(1) - (AT) L2 - art. 21(3)	art. 48(1)	art. 34(1) L2 - art. 17	L2 - art. 79(1)	art. 79(2)	L2 - art. 258(3)	L2 - art. 57(3) - A	L2 - art. 11 (2)		art. 24a 1(h)	art. 21(5)
	Contingency plans		art. 85(2)		art. 47(1)	part of BCP as referred to in art. 34			art. 41(4)					art. 21(5)
	Crisis management and communications					L2 - art. 22	L2 - art. 79(4)							
	Disaster recovery plan					art. 34(1) L2 - art. 19	L2 - art. 79(1), art. 78	art. 79(2)						
	2h RTO				L2 - art. 15(2)	L2 - art. 17(6)	L2 - art. 79(2)							
Incident reporting	Reporting of operational incidents to CAs	art. 96(1)			L2 - art. 23(3) L2 - art. 8(1)		art. 45(6) L2 - art. 43(1)							
	Procedures to record, monitor and resolve operational incidents						L2 - art. 71(4)						art. 24a 1(i)	
	Breaches in physical and electronic security measures	art. 96(1)		L2 - art. 18(3) (AT)								L2 - art. 9(4)		
Testing	Testing of IT tools, systems and procedures	L2 - art. 3(1)				partly relevant by general provisions art. 49	art. 45(5) L2 - art. 72(2)							
	Penetration testing			L2 - art. 18(4) (AT)										
Third party risk	Outsourcing - the entity remains fully responsible	art. 19(6) art. 20(2)		L2 - art. 4(1) (AT) L2 - art. 31(1)	L2 - art. 6(1)	art. 35(1)	art. 30(1)		art. 49(1)			L2 - art. 6(4)		art. 31(2)
	Outsourcing is governed by a written agreement			L2 - art. 31(3)	L2 - art. 6(4)		art. 30(2)	L2 - art.16			L2 - art. 25			art. 31(5)
	Outsourcing - report to CAs on the outsourcing	art. 19(6)			L2 - art. 6(5), (7)	art. 35 approval by CA required			art. 49(3)	art. 20(1) - A				art. 31(6)
	Identify critical service providers (CSPs) and manage dependencies					L2 - art. 18(3)	L2 - art. 68(1), (2)							
	Inform CAs on dependencies with CSPs						L2 - art. 68(5)					L2 - art. 9(5)		
	Robust arrangements for the selection and substitution of IT third party service providers						L2 - art. 79(9)							
	Due diligence when outsourcing to third party service providers			L2 - art. 31(2)										
	Outsourcing to third party service providers located in a third country			L2 - art. 32										

** The different elements of the building blocks (column 2) are illustrative and non-comprehensive.*
Legend: red cells = provisions missing in the EU financial services legislation; green cells = provisions exist in the EU financial services legislation; L2 = level 2 legislation.

ANNEX 3 – SYNOPIS REPORT ON STAKEHOLDER CONSULTATIONS

I. Overview of consultations activities

Throughout the preparation of this proposal, the Commission consulted stakeholders on several occasions and in several rounds, in particular by means of:

i) publication of an inception impact assessment (19 December 2019 - 16 January 2020)
ii) a meeting of the Expert Group on Banking, Payments and Insurance (EGBPI) (18 May 2020)
iii) a dedicated workshop on digital operational resilience
iv) an open public consultation on a "Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure" (19 December 2019 - 19 March 2020)

II. Stakeholder consultations

1. *Feedback on the inception impact assessment on "Digital Operational Resilience Framework for financial services"*

The Commission received two responses on the inception impact assessment, where respondents addressed specific aspects related to their area of activity.

2. *Expert Group on Banking, Payments and Insurance (EGBPI)*

The majority of the Member States expressed in the EGBPI meeting organized on the 18 May 2020 high support for strengthening the digital operational resilience of the financial sector through the actions envisaged along the four elements outlined by the Commission.

Member States also stressed the need for clear articulation of the new rules with those on operational risk (inside the Union's financial services legislative acquis) and with the horizontal rules on cybersecurity (NIS Directive).

3. *Workshop on digital operational resilience*

The planned workshop on digital operational resilience was cancelled due to the current context on COVID-19. Instead, a webinar on "Enabling a digital operational resilience framework for financial services" was organised on 19 May 2020 as part of the Digital Finance Outreach 2020 ("DFO") series of events. The webinar was attended by more than 240 stakeholders. Overall, stakeholders welcomed the initiative and expressed broad support for introducing a dedicated framework on the digital operational resilience for the financial sector with actions focused on the four areas outlined in the public consultation document.

4. *Summary of contributions to the public consultation on 'Digital operational resilience framework for financial services: Making the EU financial sector more secure'*

On 19 December 2019, the European Commission launched a public consultation on a digital operational resilience framework in the European Union. The consultation closed on 19 March 2020.

The purpose of the consultation was to gather stakeholders' views on the development of a potential EU cross-sectoral digital operational resilience framework in the area of financial services. The consultation aimed at gathering all stakeholders' views in particular on:

- Strengthening the digital operational resilience of the financial sector in particular as regards the aspects related to ICT and security risk;
- The main features of an enhanced legal framework built on several pillars;
- The impacts of the potential policy options.

The consultation document was structured in seven parts:

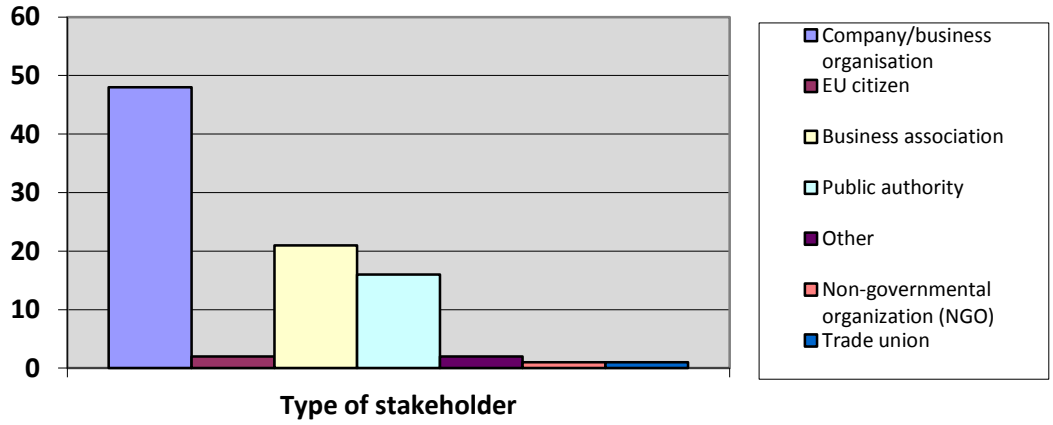
1. ICT and security requirements
2. ICT and security incident reporting requirements
3. Digital operational resilience testing
4. Addressing third party risk: oversight of third party providers (including outsourcing)
5. Other areas where EU action may be needed
6. Interaction with the NIS Directive
7. Potential impacts

The Commission received 101 responses in total, out of which 91 responses via the Have Your Say portal, and another 10 confidential responses were submitted directly via email. The feedback from the confidential responses was aggregated and anonymised to a level that prevents identification of individual entities/authorities.

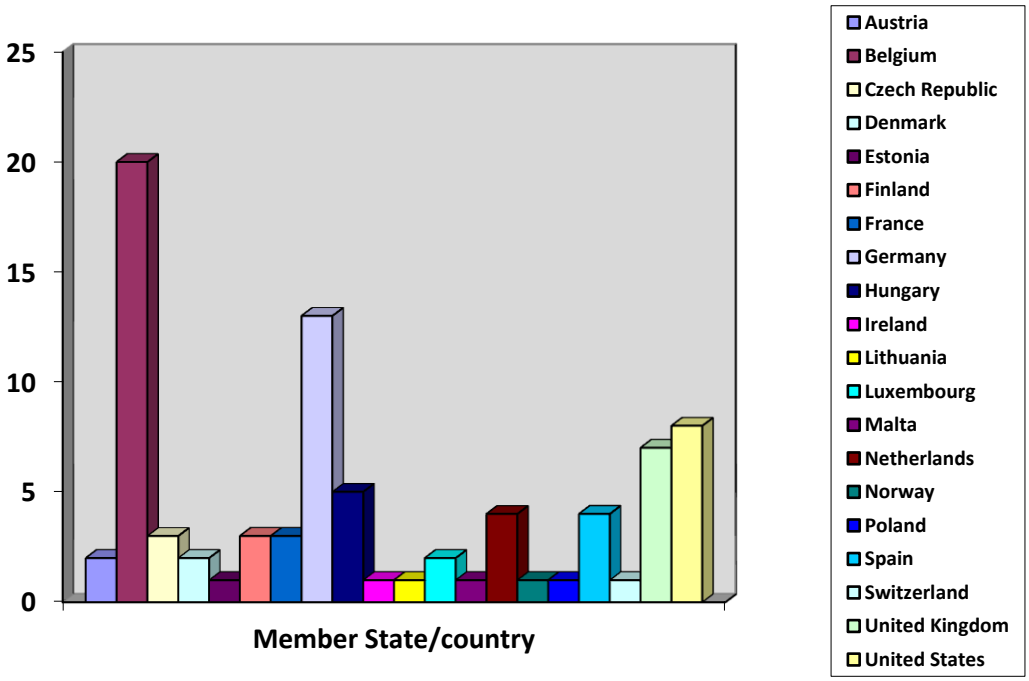
1. Overview of respondents and responses

The total number of respondents via the Have Your Say portal, and its corresponding breakdown per type of stakeholder and Member State, is as follows:

Breakdown per type of stakeholder:



Breakdown per Member State/country:



2. Summary of respondents' feedback

2.1. ICT risk management requirements

Almost all respondents agreed that *all* financial entities should have in place an ICT risk management framework based on key common principles. Most insist that these common standards should be risk-based and allow for a proportionate application, however there are some that suggest proportionality should be left out of the discussion given all players, small and large, are equally exposed to the same cyber risks and smaller ones could become the weakest entry point for attackers.

In the risk management cycle (composed, in general, by several stages designed to identify cyber risk, detect, protect, respond, recover and learn and, finally, threat intelligence sharing with other piers), most respondents faced somewhat more significant challenges during the *detection* and *response* phases. *Information sharing* with other financial actors ranks as one of the most problematic. Outside this cycle, some respondents pointed to third party risk, e.g. coordinating and auditing outsourced service supplies, differing cyber risk management frameworks and regulatory requirements, competition with Fintech/Big Tech companies that are subject to less or no requirements. When it comes to the senior management's involvement and support to manage ICT risk, most respondents rank it as quite high – Boards allocate staff, approve ICT strategies and track their implementation, and offer ICT business continuity and guidance.

The model used by large banks and insurance firms to implement ICT risk management is usually the 3 lines of defence, composed of (i) heads of unit or lines of business (risk identification and assessment), (ii) risk management units (development of the risk management framework) with a Chief Risk Officer and (iii) internal audit teams. However, small payment service providers must do the same based on EBA Guidelines on security measures for operational and security risks under PSD2.

In terms of policies or measures to identify and detect ICT risks, the vast majority of respondents (i) establish and maintain an updated mapping of business functions, roles and supporting processes, (ii) keep an up-to-date registry/inventory of supporting ICT assets, (iii) classify business functions based on criticality, (iv) map all access rights/credentials and use a strict role-based access policy and (v) deploy new ICT technologies based on a prior risk assessment. However, in some instances the maturity level of these measures could be improved.

A few large firms have faced major cyber-attacks with serious repercussions for their clients or counterparties (and themselves), details of which, however, remain confidential. Firms report that, on a daily basis, they experience cyber-attacks without serious repercussions, distributed denial-of-service (DDoS) attacks and phishing. When it comes to specifying how many cyber-attacks firms experience on average every year, responses are very diverse: some large firms mention between 10 and 20, others refer to as many as 80.000 (although not significant or creating disruptions), and payment providers mention they face thousands of attacks every day.

Almost all respondents regularly update, test and review their ICT systems and tools, and consider them appropriate to withstand cyber-attacks or ICT disruptions and to assure their operational resilience. Still, some pointed that legacy ICT systems are not constantly monitored and tested given they were not designed with security in mind, that penetration tests do not cover all critical functions, and that third party providers (TPPs) are not subject to the same requirements. Only a very limited number of respondents have not (yet) developed a cloud strategy, mostly because they chose to develop on-premise cloud technology that is specifically deployed for core business. The majority outsources to the public cloud, which they consider to be contributing to managing and mitigating ICT risks. More so, respondents use multiple cloud service providers (CSPs) based on a Board/senior management approved competence centre for cloud in each organisation.

Many stakeholders report they have legacy ICT systems that they would need to reconsider, but the level of investments needed for enhanced ICT security requirements would be significant (only one large firm indicated a number in the range of €100 millions). However, in the event of a cyber-attack or incident, most firms do not find legacy systems to cause added difficulties; the most pressing concerns are the ICT environmental complexity and lack of skilled staff. Most respondents consider to have implemented high standards of encryption, while some respondents stressed that legacy systems sometimes do not allow encryption solutions to meet the latest standards, though.

A striking majority of respondents have a structured policy for ICT change management and regular patching and a detailed backup policy. Also, the majority has established and implemented security measures to manage and mitigate ICT risks (e.g. organisation and governance, logical security, physical security, ICT operations security, security monitoring, information security reviews, assessment and testing, and/or information security training and awareness measures). Legal clarity and simplification would be most needed for the mandatory compliance audit, as well as ICT and security audit of the outsourced service providers.

All respondents consider that they have established and implemented security measures to manage and mitigate ICT and security risks. Nevertheless, a number of them indicated that they plan further improvements and significant investment programs in the next years. Some follow national or EU rules (e.g. EBA guidelines and Solvency II) or global standards (e.g.

ISO). Based on global and regional regulatory requirements and best practices, some respondents have developed their own policies, standards, and guidelines covering information security and risk. Respondents mentioned the following fields where legal clarity, simplifications or improvements would be needed: (i) the mandatory compliance audit, as well as ICT and security audit of the outsourced service providers, (ii) proportionality for smaller institutions, and (iii) information sharing practices among institutions and among regulators.

Given that most respondents from the financial sector have not yet reported major ICT incidents, or a serious/major cyber-attack, they could not give a precise answer about the time needed to restore systems. Many mentioned 2 hours while others gave the range between 0 and 72 hours. Respondents reminded that the time needed was also a function of criticality, scope of the data, ICT systems affected and the type of attack. A financial market infrastructure, which has moved to cloud solutions for its enterprise network, reported a drastically reduced number of incidents, especially concerning availability. A few respondents warned that imposing a sector critical standard for restoration time without consideration of all factors could be impractical and technically unfeasible.

Most of the respondents did not report major hurdles when trying to ensure a quick restoration of systems and maintaining continuity of business functions. Nevertheless, a number of respondents agreed that the lack of common contingency, response, resumption/recovery plans for cyber security scenarios is an issue where more financial actors in a particular ecosystem are impacted. Respondents also mentioned the following difficulties: (i) isolating and disabling affected information systems, (ii) issues with multiple vendors, and complex ICT environment, (iii) communication and reporting during the incidents, informing users about the situation, (iv) in case of a sizeable attack the mobilization of a large amount of skilled resources in a limited period of time to supplement the internal team, (v) the need to collect relevant data for further investigation, and (vi) identifying whether the attacker has managed to install other attack tools in other systems.

In the opinion of most business respondents, the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) depend on the criticality of each system, the underlying incident, and the changing requirements of every business process. It also differ across financial sectors like insurance, banking and asset management. Taking a one size fits all for approach is therefore not appropriate or even impossible and can disrupt entrepreneurial freedom, in the opinion of respondents. Others nuanced that setting clear expectation would be an advantage, as it would direct the market to a particular behaviour and improve stakeholders' trust, but meeting hard deadlines may come with a number of critical steps being lost or ignored. Most business respondents stated that legislation is not necessary in this regard. Some business respondents preferred determining RTO and RPO requirements on a risk base instead of including specific durations in legislation. One respondent recommended legislation to define non-binding RTO and RPO durations as general guidelines and only foresee requirements to uphold the functionality within specific contexts.

Respondent authorities mostly agreed with business respondents that hard RTO/RPO requirements would be counterproductive (e.g. prevent state-of-the-art cyber defence and resilience procedures). One respondent authority believed that guidance to the regulated entities is needed to ensure resilience and recovery in the case of cyber incidents and ensure more streamlined supervision and on-site inspections. Others believed that for supervisors it would be better to gain access to detailed qualitative reports, which enable critical analysis on

a much deeper level of significance and information. It was also proposed that firms be required to specify RTOs and RPOs for every service they provide to their customers.

Respondents used a number of activities or measures to incorporate lessons post-incidents and enhance the cyber security awareness within the organization. All respondents promote staff education on ICT and security risk through regular information sessions and/or trainings for employees. Respondents use online videos/e-learning, (regular) mandatory trainings, face-to-face meetings, presentations, newsletters, cyber kiosks, phishing campaigns and invitation of staff to report suspicious behaviour. Almost all respondents reported that they try to identify root causes, conduct ex post root-cause-analysis of cybersecurity incidents and prevent the occurrence of repeated incidents. The large majority also confirmed that they receive from the Board support for implementing effective cyber incident response and recovery improvement programs. Respondents also organise dedicated trainings for the Board members and senior management, who also receive reports on major incidents. Some, nevertheless, indicated that it can be difficult to gather the attention of Board members on the details of cyber risk initiatives and issues given their technical nature and members' busy agendas.

In the opinion of some respondents, risk management activities continue to be in silos at the industry level hence the financial sector would benefit from enhanced information sharing across sectors, between government and industry and among cybersecurity vendors, provided it remains voluntary. It was also suggested that the public sector could drive a common approach and culture to implementing/remediating 'after action' items from sector exercises, and brokering agreement on common communications protocol and taxonomy. More regulatory engagement was also suggested in designing threat exercise scenarios.

2.2. *ICT incident reporting requirements*

Mostly all respondents are currently subject to ICT and security incident reporting requirements that either stem from regulation (e.g. GDPR, eIDAS, national rules transposing PSD2, NIS, or other national laws), supervisory expectations (e.g. SSM, TARGET2) or industry best practices. CSPs indicated that, while they are not directly subject to incident reporting derived from financial regulation (but they are still bound by GDPR and NIS obligations), contractual terms with financial entities oblige them to report incidents to satisfy the requirements imposed on their customers. One respondent believes that the myriad of different requirements creates a significant compliance burden without a corresponding improvement in security.

The big majority of respondents agree that a comprehensive and harmonised EU-wide system of ICT and security incident reporting should be designed for all financial entities: a uniform scheme, uniform criteria and via a single reporting path. In this way, the report can be forwarded to all authorized competent authorities (which, however, should be kept small on a need-to-know basis, since reports usually contain sensitive data). Such centralisation, which is only opposed by respondent financial market infrastructures, will provide efficiency since it will allow organisations facing an incident to focus on recovery rather than on multiple reporting procedures and channels. A few respondents point to a channel of information that should go both ways: regulators should also share anonymized data on threats and vulnerabilities relating to an event to aide wider collective defence as well as individual firms' strength. One central bank considers it necessary to include ICT TTPs outside the financial system in the incident reporting scheme to facilitate cross-sectoral and cross-border communication and cooperation and to curb adverse implications triggered by cyber incidents.

Almost all stakeholders call for a harmonised taxonomy of reportable incidents, reporting templates and timeframes, and materiality thresholds. Some respondents call for a single reporting line per cross-border banking group. One central bank calls for a 2-phased harmonisation: the first phase would be focused on the harmonization of significant incidents with cross-border dimension, and the second phase would include further minor incidents. Interestingly, one respondent suggest additional harmonization to encompass a breakdown and identification of attacks outside and within the EEA.

Regarding the level of detail, respondents find it necessary to include indicators of compromise, the scale of the attack (including geographical impact and number of users impacted, if any), type of incident (based on the ENISA Incident Classification Taxonomy), timing of the incident, steps taken to rectify it, current situation in incident resolution, projected timeline for return to normal operations, impact on critical services and, possibly, lessons learnt. Some recommend a phased approach, allowing for an initial incident notification of information that is actually reliably known or feasibly available at the time, followed by a subsequent report based on the evidence found post-mortem.

Most respondents consider that materiality thresholds for incidents should be established, and some suggest criteria such as risk to the security of supply or to the stability of the financial system, or impact of the incident combined with the intention behind it (if targeted and malicious). One central bank recommends leaving materiality to national discretion, other that all incidents should be reported to avoid blind spots – the more data, the more awareness.

Few respondents consider it necessary to add new governance elements such as a CISO around ICT and security incident reporting. Reporting to a single national authority would be desired. More than a third of respondents, and notably CSPs and payment service providers, support exploring the set-up of an EU central hub entrusted either with receiving the reports and automatically notifying national competent authorities or with centralising reports forwarded by the national competent authorities to fulfil a coordination role. Respondents suggested the central hub could be the ECB, EBA or ENISA. However, to be noted that most central banks do not welcome the idea of a central hub.

The big majority believes EU legislation should establish a standing mechanism to exchange incident reports among national competent authorities, but warn that sensitive data should be kept confidential. Some point that an EU authority acting as a central hub would remove this issue. Many respondent competent authorities advise not to create parallel mechanisms in the NIS Directive and the financial supervisory framework.

Lastly, respondents find there are many factors that hinder cross-border cooperation on ICT and security incidents, and they point to differences in national legislations and supervising practices, the fragmented implementation of the NIS Directive requirement for reporting, requirements around critical infrastructure in local jurisdictions, business competition, data confidentiality, data privacy (GDPR obligations), fear of reputation damage and risk of leakage of potentially compromising information.

2.3. *Digital operational resilience testing*

The overwhelming majority of respondents that provide financial services are already required to carry out ICT or security testing. Respondent authorities such as central banks and supervisory authorities also mandatorily test their ICT resilience. Few respondents (e.g. CSPs) are however not subject to such requirements. On top of requirements, the overwhelming

majority of respondents, businesses and authorities carry out ICT or security testing on a voluntary basis.

The majority of firms face issues with overlapping or diverging testing obligations. Companies with locations in multiple legal systems are often confronted with overlapping requirements for ICT and security tests by different authorities, which tie up considerable resources. Therefore, these respondents believe that harmonizing the requirements for ICT and security tests, reducing compliance complexity by integrating regulatory guidance, expectations and requirements would benefit both companies and authorities.

The majority of respondents agree that financial entities should be required to perform a baseline testing/assessment of their ICT systems and tools. They also found useful all of the proposed methods (e.g. gap analyses, compliance reviews, vulnerability scans, physical security reviews and source code reviews). Respondents also suggest business continuity tests, disaster simulations, penetration-testing, standard app and network security assessments, DAST, open source analysis, bug bounty programs, red teaming, and vulnerability assessments.

Respondents propose that testing should be proportionate, based on the risk profile, sector, size, scale, complexity and location. Others noted that the choice depends on the criticality and the circumstances and if own systems or third-party systems are used. Some respondents recommend a uniform testing framework with quantitative results that are empirically analysable and comparable across Member States. Others warn that duplication of testing at EU level with national level should be avoided, but convergence of terminology and practices (based e.g. on ISO) would be welcome. Some respondents warn that regulatory-led tests (or unknown third-party testers) can expose the firm to undue risk, hence proposed using own staff and/or firm-approved vendors. Finally, flexible testing, which can adapt to the rapidly evolving risks of the financial sector, was preferred.

The overwhelming majority of respondents agreed that more advanced testing should be carried out for significant financial entities identified at EU level or designated by competent authorities. They supported all criteria for identifying significant entities such as proportionality related factors (i.e. size, type, profile, business model), impact related factors (criticality of services provided), and financial stability concerns (systemic importance for the EU). They also proposed other criteria such as the amount of personally identifiable and/or financial data, interdependencies with other sectors, and historical records of material cybersecurity incidents. Some mentioned that even small entities could cause significant effects (due to interconnection) depending on the criticality of their services to the financial system. Some respondents suggested not developing an additional and potentially overlapping list of ‘significant’ institutions but using existing lists (e.g. based on NIS, SSM). Finally, some respondents suggested that national authorities rather than EU level bodies should select significant institutions.

The majority of respondents preferred that more advanced testing (e.g. TLPT) not cover all functions and remain not compulsory. Some respondents (both businesses and authorities) argued that TLPT testing is not necessary for ensuring digital operation resilience; it is costly and should be carried out only for significant institutions. The majority agreed that testing should focus on live production systems (while avoiding disruption to live services) and testers be certified based on recognised international standards. Respondents were more split on whether the financial entities should employ their own (internal) experts that are operationally independent in respect of the tested functions. Some argued that mandating

internal experts to carry out testing would be impractical and burdensome for financial entities. Both businesses and public authorities supported that tests run outside the Union be recognised as equivalent if using the same parameters (and thus be held valid for EU regulatory purposes). The majority of respondent financial service providers and public authorities supported one testing framework applicable across the Union and that ESAs be directly involved in developing a harmonised testing framework (e.g. by issuing guidelines, ensuring coordination). Still, some argued that national competent authorities should oversee the harmonised testing principles and requirements, but should not be directly involved in running the tests.

There was no consensus among respondents about the most efficient frequency of running more advanced testing. While many supported annual testing, about the same number of respondents proposed 2 or 3-year frequency. Many respondents believed that it is not possible or advisable to determine a general frequency for all. Many argued that the frequency of advanced testing should be determined based on the overall situation of the financial institution, its size, risks and existing or potential threats. Furthermore, different types of tests need different frequency. They warned that advanced testing is expensive, requires large internal and external resources and takes months. One respondents argued that in-house red team tests should be annual, while tests which involve external testers and regulatory oversight should take place once every three years. Others advised that penetration testing should occur annually or after significant changes, scanning needs should occur quarterly and critical functions may be tested more regularly. Finally, it was also mentioned that legislative requirements for testing frequency could reduce the flexibility of authorities and firms to prioritise cutting edge methods of monitoring risk and resilience in the future.

Most respondents agreed that both the baseline testing/assessment tools and more advanced testing (e.g. TLPT) can have a prudential impact for financial entities when they make updates based on the results. Operational testing can act as a catalyst for more cyber resilience and thus contribute to overall financial stability and business development. One respondent suggested having an EU recognized certification in place – in a recognized and global framework with internal team certifications. Others advised to use existing guidance and frameworks (e.g. IST, SANS, TIBER-EU) to build on.

2.4. *Addressing third party risk: oversight of TPPs (including outsourcing)*

In their responses, stakeholders pointed out they already use a number of ICT TPPs such as software and hardware providers, data centre hosting and CSPs, internet/ network/ telecommunication providers, cybersecurity protection service providers, IT operations, business process operations, infrastructure operations, payment transactions processors, payment gateways, clearing houses, card schemes, customer onboarding service providers, outsourced development and public services.

The provision of cloud technology-enabled financial services is highly dependent on data. According to one respondent, a typical European financial institution accesses over 1,000 different cloud services, many unapproved and unlikely to be monitored. Employees and partner organisations may use ICT systems that are not monitored, managed and secured. These third parties could increase operational risks greatly; however, the competent authorities' oversight over some ICT (cloud) TPPs are inadequate. Some relevant ICT TPPs are not regulated within the EU. One respondent advised the EU legislation to make it clear that organisations are responsible for all aspects and behaviour of all employees, sub-contractors and business partners, whatever ICT services may be in use. Another respondent

highlighted that an effective vulnerability assessment program should include the identification and management of risks introduced by third party vendors and software. Good practices could include automated scanning software and services for third party risk management, because assessment questionnaires do not sufficiently provide an accurate picture of underlying risks or vulnerabilities

Most respondents have experienced difficulties during contractual negotiations with ICT TPPs. They pointed out to several aspects as being difficult to negotiate, such as for instance: (i) ICT and security related legal obligations imposed by the national or EU supervisory authority (e.g. 2019 EBA Outsourcing Guidelines), (ii) regular and mandatory audit clauses /right to audit (especially with the larger global CSPs), (iii) geographical storage of data (e.g. GDPR requirements), (iv) sub-contractor approvals, (v) customer and its external auditors subcontracting information and control rights, (vi) information rights, (vii) exit strategies for SaaS products, (viii) post-termination assistance, (ix) resolution requirements under BRRD directive, (x) business continuity clause, (xi) penalties for non-compliance with SLAs and (xii) transparency on processing orders to subcontractors and outsourcing chains that lead abroad, etc.

CSPs offer their highly standardized scalable services to many different clients. Hence, they generally do not cater for individual specifics of industries. One respondent added that the situation is even more difficult where the vendor is not itself a CSP, but subcontracts to a CSP as the intermediary has no ability to alter a CSP's terms. Nevertheless, another respondent reassured that, usually, the bigger, more professional TPPs are compliant with supervisory/regulatory authorities when it comes to contractual negotiations. Finally, while larger institutions are able to secure certain concessions from the provider, smaller institutions may face challenges in securing similar outcomes.

A CSP reported about historical difficulties in contract negotiations when requirements have not considered the nature of cloud services (e.g. the specificity of the multi-tenant environment). However, the EBA cloud recommendations, its outsourcing guidelines and EIOPA's outsourcing guidelines have significantly helped to address these difficulties as they recognise and account for the specificities of cloud. This was also confirmed by a public authority, which perceives significant developments regarding the outsourcing contracts of the undertakings, thanks to the useful international and national guidelines.

It was also highlighted that certain jurisdictions in Europe have more stringent requirements for outsourcing and require certain data localization or pre-approvals from regulators, which may be in conflict with other laws, e.g. the GDPR and the current EU-wide initiatives for the free flow of data. The lack of standardization in controls, processes, and reporting across industry results in unnecessary complexity and frustration for both financial institutions and third parties. A respondent recommended introducing a Standard Certificate Framework (substituting detailed auditing of the legal compliance), which would be commonly and mutually accepted by all European and national supervisory authorities. It was also argued that voluntary minimum Standard Contractual Clauses would establish a clear guideline for CSPs on the implementation of financial institutions requirements in their services and would reduce the burden to negotiate contracts for individual financial institutions. It was also raised that banks face challenges with the limited amount of CSPs, which in the long run might lead to the build-up of systemic risk/instability as the CSPs might not have the resources to help all their financial clients, if their cloud system breaks down at once.

Some respondents supported the implementation of Standard Contractual Clauses for cloud arrangements on a voluntary basis while others argued that they should be mandatory. It was also argued that due to the market power of the CSP, a standard contract should be drawn up at European level. Nevertheless, a number of respondents expressed that the new EBA/EIOPA outsourcing guidelines already adequately define supervisory requirements for outsourcing and provide clarity. Any standard clauses should provide the necessary clarity or elaboration to give effect to the requirements set out in outsourcing guidelines and to ensure that relevant obligations are appropriately reflected in outsourcing arrangements. In the opinion of some respondents (both businesses and authorities), further standardization of contractual clauses should continue to be risk and principle based.

SCCs should be limited to regulatory minimum requirements as an attachment to otherwise freely negotiated contracts, including service content, accompanied by clear supervisory guidance to avoid inconsistent interpretations. The complexity and variation across both financial entities and service providers (Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), and hybrid cloud environments) makes it nearly impossible to provide a "one size fits all" contracting solution. Furthermore, introducing SCCs should not create additional regulatory and operational complexity for firms (extensive renegotiation), reduce competition or increase in the costs.

In their replies, respondents pointed out to several clauses that could be useful for the Commission's work on SCCs for cloud arrangements with financial sector entities. For instance, their suggestions include (i) rights to audit and access (timing, scope, auditor, publication), (ii) supplier obligation to notify and provide audit reports, (iii) supervisory examinations, regulator relations to suppliers, use and risk management of subcontractors, (iv) (v) data portability and exit strategies, (vi) data location and transfer (with protection or limitation within EU), (vii), sub-contractor authorization, (viii) notification in case of significant incidents, etc.

CSPs also listed the requirements that do not lend themselves to standardization: description of the services, fees, security measures, certifications and audit reports, SLAs, and insurance. In their opinion, the following aspects can be part of standardisations: regulator/customer information, audit and access, business continuity and disaster recovery, significant developments, chain outsourcing. They warned, however, that standard contract provisions should not be detailed or prescriptive.

Business respondents also suggested that any such standard clauses should also be available for TPPs to use with any sub-processors, and should be harmonized with data processing standard clauses under the General Data Protection Regulation (EU) 2016/679 (GDPR).

An overwhelming majority of respondents supported the introduction of an oversight framework for ICT TPPs. The majority of respondents agreed that it should focus on critical ICT TPPs and "criticality" be based on a set of both qualitative and quantitative thresholds (e.g. concentration, number of customers, size, interconnectedness, substitutability, complexity, etc.). They also thought that proportionality should play a role in the identification of critical ICT TPPs. A variety of aspects such as data portability, exit strategies and related market practices, fair contractual practices, environmental performance, etc. should be included in the oversight framework.

Respondents mostly supported, but a number of them rejected, the idea that EU and national competent authorities responsible for the prudential or organisational supervision of financial

entities carry out the oversight. In some opinions, not all regulatory authorities today have good capabilities, resources, expertise of the more technical aspects of ICT services; rather better cooperation with industry would be welcome. Even authorities questioned if supervision is capable to guarantee sound and secure ICT by licensing regime.

Fewer respondents managed to form an opinion on whether collaboration mechanism e.g. within colleges of supervisors should be established but most of them would support such a solution. It was also suggested that not the NCAs but a European organization should be responsible with sufficient mandate and authority to perform this task as mostly large, global service providers are in scope. The oversight framework and body should be cross-sectoral (insurers, banks, asset managers, market infrastructure operators all using the same providers and range of products). An extension of the remit of existing authorities such as ENISA or BEREC, or a new focused Authority, was also proposed to be used.

Respondents also highlighted that any oversight framework should be coordinated globally due to the interconnected nature of financial services and service providers. An EU-specific oversight framework for ICT providers may harm the competitiveness of European firms by potentially limiting the range of third parties they are able to partner or outsource certain functionalities to.

Most respondents (both businesses and authorities) rejected the idea that the oversight tools should be limited to non-binding tools (e.g. recommendations, cross-border cooperation via joint inspections and exchanges of information, onsite reviews, etc.) and would rather support binding tools (such as sanctions or other enforcement actions). Nevertheless, a number of banks, payment service providers and authorities would support the non-binding tools and rejected the idea of binding tools.

CSPs understand regulators' concerns, however they think that introducing direct oversight over TPPs could create technical and regulatory complexity that need to be addressed beforehand. They proposed to consider conducting gap analysis of the existing outsourcing frameworks to understand how they could be strengthened, and introducing (i) harmonised regulatory guidance on assessment of criticality and importance of outsourcing to CSPs, (ii) consistent cloud audit framework and considering if audits should be performed centrally, including by regulators directly, (iii) joint critical incident reporting taxonomy between the financial institutions and their providers based on common principles, templates and thresholds. Direct oversight over TPPs raises a number of questions and issues in terms of e.g. scope, technology neutrality, updating, variety of customers and services, proportionality, criticality, competent authority and its expertise. In some opinions, the existing legislative initiatives already undertaken and underway e.g. NIS Directive, GDPR, Electronic Communications Code, Cybersecurity Act are sufficient. They warned that the regulatory oversight landscape for ICT providers should not become too complex, unworkable, and serve as a market entry barrier for smaller providers.

Both businesses and authorities rejected the listed possible solutions to address concentration risk among ICT TPPs. Most of them did not support either diversification strategies (mandatory or voluntary rotation), a mandatory multi-provider approach or exposure limits. Mandatory rotation may cause inconsistent quality and significantly increase organizational overhead to deal with a new level of complexity. Furthermore, IT rotation has more transition costs and takes much longer than rotation of financial auditors. Mandatory multi-provider approaches would significantly increase costs and add complexity to everyday management. Diversification and portability may not be achievable in case of a high degree of reliance on a

specific ICT third party provider (e.g. custom solutions). Limits would be impossible to implement in the real world. Binding methods can hinder the ability to continuously improve one's resilience and to adapt to new business models and technologies.

CSPs believe limitations would restrict the ability of financial entities to select their provider based on risk assessment and preferred service offerings. They warned that multi-cloud management layers can present challenges to operational resilience, significantly increases operational complexity and risks, as well as costs. Rotation of CSPs (mandatory or voluntary) would be disproportionate and not feasible either technologically or commercially. Regulators and policymakers could facilitate development and sharing of best practices (on e.g. business continuity and disaster recovery procedures, multi-cloud and portability strategies) and later consolidate them in an operational resilience guidance. In the long run, financial institutions may build multi-cloud strategies and re-architecting for a multi-cloud ecosystem, but technology development is not there yet, and prescriptive legislation would not be practical.

In the opinion of some respondents, concentration risk can be better addressed by (i) regulating CSPs' conduct and enforcing their fair competition (foreign-based providers be held accountable in the EU) (ii) fostering standardisation and interoperability (e.g. through open interfaces, data formats or proven migrations) for seamless portability of data and applications and multi-cloud approaches and/or exit strategies, (iii) allowing diversification of risks globally by removing data localisation rules whenever possible, (iv) lowering barriers to market entry and helping smaller providers to scale up, and (v) requiring excess capacity for at least one critical system to be included in the contract for critical TPPs. Given the fragmented nature of the landscape, regulatory oversight may need to wait until cloud adoption and penetration of critical outsourcing becomes widespread.

2.5. *Other areas where EU action may be needed*

Information sharing

The majority of respondents agreed that the EU should have a role in supporting and promoting the voluntary information sharing between financial institutions and that this could be extended to other industry sectors. Many respondents already participate in cyber-threat information sharing platforms such as the FS-ISAC, CIISI-EU, FSISAC EU, WFE GLEX, FSCCC (in UK), TCO Advisory Group Cyber (in NL), etc., which, in their opinion, work well. Most respondents argue that the EU can further support such information sharing by providing legal protections from liability and incentives for companies to participate. In this context, both businesses and authorities considered that the financial sector would benefit from a stronger role of ENISA.

Respondents indicated some challenges for threat intelligence sharing related to concerns around data confidentiality and data privacy, certain law enforcement restrictions that prevent cross-border information flows, competition law, reputational damage, trust, and national security concerns related with financial stability or critical infrastructure protection.

The opinion of the majority of the respondents is that cross-border information exchange can help reduce information asymmetries across jurisdictions, and foster coordination, communication and cooperation among authorities. A few diverging opinions question the added value of such platforms, however, arguing that the existing level of sharing amongst financial institutions is very high.

Promotion of cyber insurance and other risk transfer schemes

Most respondent businesses have cyber insurance or risk transfer policy, either in the form of a standalone cyber-risk insurance policy or bundled policies. Some reported that their policies cover liability arising from cyber risks and the delivery of products and services, while others are only covered for disasters or very major incidents.

It was noted that insurers have a key role to play in increasing cyber resilience, not only by providing risk transfer or cyber cover, but also in helping their clients identify vulnerable business functions and practices, preventing cyber risks and mitigating their impact when they materialise (e.g. forensic IT services and legal support). Nevertheless, respondents warned that insurance programs are in no means expected to replace existing firm capabilities to respond and recover from cyber incidents.

In the opinion of some respondents, a cyber insurance policy should cover cost to recover a serious breach, extortion, electronic compromise and social engineering. Cyber insurance should be premised on the presence of effective risk management tools including a scanning and vulnerability management program. In the opinion of an insurer, standalone cyber insurance should be offered on a first and third party basis as first party claims can become third party claims very quickly and vice versa. Some business respondents agreed that combination of both first and third party liabilities is the optimal coverage.

Respondents agreed that (i) the lack of a common taxonomy on cyber incidents, (ii) the lack of available data on cyber incidents, (iii) the difficulties in estimating pricing or risk exposures and (iv) legal uncertainties around the contractual terms and coverage pose challenges for the development of an EU cyber insurance/risk transfer market. However, respondents were split on whether the lack of awareness on the importance of cyber/ICT security would be an issue.

In the opinion of an authority, cyber insurance is still a rather underdeveloped area compared to the mainstream insurance products. Lack of demand is related to a low awareness of businesses and individuals about the cyber-attack risks and losses and the lack of knowledge about cyber risk management procedures. Lack of supply on the part of insurance companies come from the fact that cyber risk is difficult to quantify. Business respondents agreed that lack of data on cyber-incidents as well as the problems and complexity of estimating the cost of exposure to cyber-risk and ICT risk were the most important challenges. Others highlighted that the lack of data most importantly related to extreme cyber risks (tail risks) cause biggest difficulties in pricing and risk management.

An insurer argued that the most important hurdles for cyber insurance becoming a mainstream product is that cyber risks are difficult to quantify and assess, largely due to a lack of good quality data. In particular the following factors matter: (i) uncertainty of potential future losses, (ii) highly correlated risks due to widespread use of certain operating systems, software or cloud computing services, (iii) multiple (affirmative and/or non-affirmative) guarantees may be triggered in different lines of business, (iv) a lack of available data on cyber incidents and losses, (v) increasingly intangible losses.

It was also noted that, given the evolving nature of cyber risk, any fixed taxonomy for reporting could quickly become meaningless. Qualitative risk is difficult to measure for insurance firms as there are substantial variables to measure risk profile, and these can vary

substantially between entities. The qualification of cyber incidents resulting from warfare, state sponsored attacks and ransom demands is also an issue.

Respondents mostly supported that the EU provides support to develop EU or national initiatives to promote the development of the cyber insurance/risk transfer market. The EU can bring together providers of threat information, security companies, insurance providers and support the development of different risk models on the basis of known threat information or disclosed incidents/damages. An insurer suggested that the EU could support awareness raising, by supporting the development and provision of cybersecurity training programmes for businesses. It was also proposed to have an elaborated approach to the prudential recognition of cyber insurance/risk transfer as a risk mitigation control.

In some respondents' opinion, the EU should provide statistics and a better documentation of attacks. Industry initiatives, where cyber event data is pooled and exchanged via a platform (similar to PERILS for natural catastrophes event data) should be stimulated, which would simplify application and process architectures of financial organizations and allow better pricing and risk management under more certain conditions. Cyber-incident data already gathered under the GDPR and the NIS Directive could also be used as a basis.

In the opinion of an authority, as the first step, the EU could support the creation of a common taxonomy for cyber incidents to better set up data collection systems and also to understand the collected information. Others noted that taxonomy for cyber incidents has already been defined by the CRO Forum. Existing European initiatives (e.g.: ESRB's European Systemic Cyber Group taxonomy and classifications on Systemic Cyber Risk) would also be useful for developing risk transfer and mitigation mechanisms.

2.6. *Interaction with the NIS Directive*

A majority of respondents indicated that they fall under the scope of the NIS Directive, mostly by virtue of being designated as an operator of an essential facility (OES) or as a digital service provider (DSP), or as an authority in charge of identifying NIS entities. As regards the former, most firms fall in one of the three financial sectors within the scope of NIS (credit institutions, trading venues and central counterparties). In addition, some firms (notably in the area of insurance) are subject to NIS as a result of the scope being increased when transposed nationally.

As a result of falling under the scope of NIS, they become subject to security controls and incident reporting/notification obligations. However, in some Member States, there is no additional reporting, as reporting to financial regulators is deemed equivalent. DSPs also flag being subject to additional requirements (e.g. technical and organisational measures).

Some respondents stress that the NIS directive has established a common baseline and a common frame for ensuring that operators of essential services can respond to attacks and recover. They also stress the importance of the Computer Security Incident Response Teams (CSIRT), also as a base for international cooperation. Some respondents also stress that being within the NIS universe is good for financial firms, as they can learn from experiences in other sectors.

Respondents highlight that Member States have implemented the NIS directive unevenly and inconsistently. Some respondents (mainly companies) argue that this creates significant problems for cross-border firms operating across the internal market. Others, while acknowledging issues of different implementation, nevertheless stress that detailed

consistency is not necessary but that it would be more important to close gaps and address weaknesses to improve Europe's capacity to respond to large cyber-attacks.

As regards the impact of NIS on firms and the sector as a whole, respondents paint a nuanced picture. Some respondents from the private sector (companies, associations), argue that the *impact on firms* has been limited, given pre-existing requirements in financial regulation either stemming from national or European legislation that were largely similar or more ambitious compared to NIS. While agreeing that the impact has overall been quite limited on firms in the financial sector, many respondents nevertheless stress that NIS has established additional requirements on top of financial regulatory ones related to audit obligations vis-à-vis National Security Authorities (NSAs) and double reporting of operational and security incidents to NSAs. These are made more burdensome by differences in national implementation. As regards the *impact on the financial sector*, some respondents stress a positive impact in terms of increased monitoring and awareness of security incidents but also stress a negative impact in terms of reporting overlaps and associated high costs.

Public authorities in particular stress the impact in terms of institutional structure, with the creation of CSIRTs. In terms of substance, many respondents stress a limited impact either because of the *lex specialis* clause or because pre-existing national rules already addressed operational and security risks to a similar extent. One respondent also stressed that the limited effect is also due to the limited scope of NIS in terms of financial sectors, arguing that it does not establish a comprehensive regime for the financial sector, largely overlaps with financial sector rules on ICT risks and accordingly imposes regulatory burdens without much effect.

Many respondents further stress that they are subject to more specific requirements compared to the ones set out in NIS. As regards respondents from the *private sector*, a large majority stress that they are subject to more specific requirements in particular as regards reporting and ICT risks. These stem from national rules, EU rules and supervisory requirements. As regards EU rules, respondents mention in particular PSD 2 (e.g. Article 96), MiFID, CSDR, Solvency 2, as well as more generally GDPR. Public authorities also stress additional organizational and technical requirements stemming from national laws on cyber security; additional rules stemming from EU financial regulation as regards IT security rules and requirements; and supervisory requirements (e.g. European System of Central Banks).

On potential issues stemming from NIS competent authorities being different from financial sector competent authorities, some *private sector* respondents argue that it is not a major issue, even though it would be convenient to have one authority in charge of both. Many respondents nevertheless stress that parallel and overlapping supervision increase compliance efforts. One respondent stress that the differences are significant, as the way the NIS directive has been transposed is often been modelled on preexisting national rules that are cross-sectoral, national interest focused and outdated. Some public authorities stress problems in terms of information sharing, resulting in limited central knowledge of security incidents. Others nevertheless stress that cooperation between authorities is regular and occurs on a "need-to-know" basis.

As regards the way firms cooperate with NIS authorities, *private sector* respondents paint a mixed picture. Some stress that ways to cooperate is set out in law, and hence not based on agreements, whereas others stress that cooperation is more informal. One respondent also stress that as a result of the NIS Directive, NIS authorities have to cover many more firms without a matching increase in resources, and as a result, interactions stay at quite a generic level.

Public authorities provided answers to additional questions (52-56). As regards whether they receive relevant NIS information and if so in what way, respondents had different views. Those who are designated as NIS authorities naturally received information, stressing that they shared it with other authorities, if necessary with financial supervisors, also in light of MoUs. Those who are not NIS authorities stressed that they did not receive information directly, instead relying on e.g. structured cooperation with NIS authorities, or voluntary exchange of information (often easier to orchestrate at national level). One respondent stressed that it could use preexisting information stemming from prudential supervision and oversight to get an overview.

Considering whether there is merit in national or EU financial supervisors being responsible for supervising ICT and security risks, respondents expressed different views. Some argued that NIS has already been transposed that way, whereas one responded argued that divided responsibilities do not create problems. Another respondent stressed that sharing responsibilities and establishing comprehensive cooperation mechanisms would be more useful. However, other respondents stressed the benefits of ensuring that financial supervisors are in charge, given e.g. the special nature of the financial sector (already acknowledged in NIS recitals) and the ensuing need to have a clear EU level financial supervisory regime. One respondent argued in favour of national competent authorities being in charge, while another respondent also stressed the need to clarify responsibilities between National Competent Authorities (NCAs) and National Central Banks (NCBs). Respondents in favour of financial supervisors being in charge nevertheless acknowledged the need to cooperate with other authorities.

As regards potential difficulties in getting access to information reported under NIS, most respondents argued that they did not encounter major difficulties. One stressed that access was not the issue, but rather inconsistent and uncoordinated incident reports as well as NIS limited scope in terms of financial sectors and firms. Some respondents did not express a view, arguing that experiences with NIS are so far limited, as it has just been/is about to be transposed. One respondent stressed that one problem was that the "need-to-know" basis for sharing information is not sufficiently defined.

As regards potential difficulties of cross-border coordination, most respondents responded no. One respondent stressed that the ECB has developed a framework for international cooperation for Significant Institutions as part of its incident reporting (however, no such thing for Less Significant Institutions). One respondent stressed that such issues may arise in the future, as more firms will share ICT in many Member States. One respondent also stressed that e.g. harmonised communication protocols could facilitate coordination.

As regards experiences with applying the *lex specialis* clause, respondents expressed different views. Some argued that they had no experience, as not reflected in national rules. Some stressed that it was in place in their jurisdiction, but that it had not managed to avoid duplication/overlaps and inconsistencies notably as regards incident reporting. Others argued that it worked well, notably as regards PSD2 where cooperation was deemed fluent.

2.7. Potential impacts

A majority of respondents considered that the initiative would contribute to the overall financial stability, improve understanding of firms' vulnerabilities, and increase consumer confidence and the overall operational resilience in the financial sector. The society as a whole would benefit of increased trust in the financial services industry.

Most respondents stressed that the future framework should be principle based and risk oriented, and it should encourage innovation in financial services. The rules should be proportionate to the nature/size/complexity of the entities in the financial sector. Many respondents indicated that overly detailed requirements would have a negative impact on regulated entities (e.g. increase in compliance costs), in particular for smaller and medium sized entities.

Respondents considered that close cooperation among competent authorities, better information sharing among market participants regarding cyber threats, and more investment into effective cyber defences could bring positive impact on business development. They also highlighted that an effective incident reporting and management system will certainly have a positive impact on the wider economy.

Several respondents highlighted that a supervisory framework for ICT TPPs is expected to deliver significant benefits to the industry, investors and EU competitiveness at large, and would substantially improve resilience of financial institutions, leading to the entire business environment being more secure/resilient.

An overwhelming majority of respondents considered that streamlining the existing incident reporting requirements and establishing specific arrangements to promote effective information sharing on ICT and security threats among financial market participants would bring most benefits and value for their organisation and the financial sector. At the same time, a majority of the respondents found significant benefits in establishing specific rules that enable a better oversight of certain critical ICT third-party providers and harmonising regulatory requirements on ICT and security based on international standards and best practices. Some respondents called for better cooperation among national supervisory authorities and an improved framework for cyber resilience that also leverages on international cooperation, where possible.

There were split views among respondents on the specific measures that would be completely new for them and would require a gradual approach in their implementation. While, many respondents stressed that these measures already exist in their practice (although in some cases the depth might be different), some respondents identified threat led penetration testing as requiring a transition period of appropriate length. Similarly, one public authority indicated that the measures themselves are not new, but an increased activity would require additional resources. Other respondents highlighted that specific legislation for RTO and RPO, prescriptive requirements for TLPT and requirements to limit the concentration of ICT TPPs would also be problematic for entities to implement.

A majority of respondents would expect their organisation to put most efforts in (re)training and hiring of cyber security experts, as well as in increasing workforce awareness. They also stressed that cyber security is a dynamic process and there are always developments in the threat landscape. Therefore, the baseline will always be in a state of evolution, to ensure the constant update of tools and procedures to be able to identify, detect, respond and recover from cyber security incidents.

Some respondents also expect an increase in management attention and involvement. Most organisations are continually increasing their IT budgets in areas of technology, educational training, board governance, etc. For instance, one financial market infrastructure pointed out that investment linked to the upgrading of their legacy systems, for example, is expected to turn around €100 million.

Many respondents also highlighted they are moving more services to cloud based environments and this comes with increased spending on technical and audit controls. Many efforts will also probably be required in fulfilling the testing requirements (TLPT, source code review, etc.) and compliance documentation.

In terms of the administrative formalities that are most burdensome, human-resource intensive and cost inefficient, an overwhelming majority of respondents indicated that the multiple incident reporting to various supervisory authorities, under different regulations and legislations is a serious challenge for them. A big financial market infrastructure responding to the questionnaire, estimates that the administrative cost to manage divergent regulatory requirements, ranges between 8 and 10% of their cyber security budget. Moreover, fragmentation in incident reporting leads to an additional administrative cost of around 2%.

Similarly, a majority of respondents stressed that the costs linked to the multiplication of TLPTs are also very problematic, as it is the compliance with the many regulations issues by several national and EU supervisory bodies. One respondent, estimated the cost of a security test in the range of €30 – 50.000 for non-financial firms, while for companies in the financial sector, the cost may range between €250 – 500.000 for one test. The cost of security testing very much depends on the size of the information system being tested and the particular method of testing.

Respondents also stressed the amount of surveys, questionnaires, compliance assessments and information requests they receive, and which are many times overlapping significantly and not leveraging the existing frameworks in the industry. The task of assessing and monitoring the effectiveness of the risk management frameworks of critical ICT TPPs (especially in the case of foreign service providers which are subject to different legislation) for operational resilience risks is also a complex process that regulated entities have to perform. One respondent indicated that it would be helpful if these requirements or compliance assessments were focused under one single body.

Finally, with regards to the costs incurred due to ICT incidents, respondents estimated them in terms of direct and indirect costs, however in their replies they preferred not to disclose any figures.

ANNEX 4 – DETAILED PROVISIONS UNDER THE RETAINED OPTION

The table below describes the detailed provisions under the retained option, giving an indication on the possible *core requirements* it might entail in practice for the different financial subsectors. It also provides a general indication of the status quo for these provisions in the different financial subsectors.

Table 8 – Overview of main changes to the building blocks between the baseline and preferred option

Retained option	Status quo	Under preferred option	Comments on impact
ICT risk management			
Baseline requirements	The EU financial services legislation covers the following aspects through specific provisions for the below subsectors. For those not mentioned in the list, provisions are either too general or inexistent. • *Governance*: payment service providers, investment firms, CCPs, CSDs, re(insurance) and asset managers. • *Protect:* all subsectors, except credit rating agencies. Credit institutions are covered under the NIS Directive. • *Identify, detect, change management, learning and evolving:* no subsector covered by specific measures. • *Response:* all subsectors. • *Recovery:* CCPs, CSDs, trading venues and trade repositories. For more details, see **Table 7 in Annex 2**.	The preferred option foresees the enactment of a comprehensive single framework for the digital resilience of the financial sector through the combination of different -yet related- elements. **New risk-based principles** covering the below aspects in those subsectors where currently inexistent or too general (see left column on status quo). The principle of **proportionality** would apply when calibrating these provisions for the different subsectors and types of financial institutions. • *Governance:* may include ICT risk management framework and ICT risk management strategy, defining roles and responsibilities for the Board of Directors and Senior Management for managing ICT risks, etc. • *Identify*: may include identifying critical functions, activities, products, and services and assess their respective ICT risks, etc. • *Protect*: may include tools, measures, controls to prevent, limit or contain the impact of a potential cyber event on critical functions, information assets and data, etc. • *Detect*: may include establishing capabilities to monitor and detect anomalous internal and external activities and events related to ICT risks, assess the magnitude of those events, etc. • *ICT change management:* may include establishing processes to ensure that all changes to ICT systems are assessed and implemented in a controlled manner, etc. • *Response*: may include processes and procedures to respond to an incident, mitigate its effects, business continuity, contingency	Minor changes foreseen for those subsectors in which specific requirements already exist. More substantial changes for those subsectors subject to general requirements.

		planning, etc. • *Recovery*: may include processes and procedures to repair and restore systems or assets affected by an incident and resume operations, etc. • *Learning and evolving*: may include training of staff, awareness campaigns, updating procedures and processes after incidents, etc.	
Incident reporting and information sharing			
Incident reporting	The following financial subsectors are subject to requirements on ICT-related incidents notification under the EU financial services legislation: payment service providers, investment firms (only those performing algorithmic trading), trading venues and CSDs. The following horizontal legislations contain requirements to notify incidents: NIS Directive and it covers credit institutions, trading venues and CCPs. For more details, see **Table 7 in Annex 2.**	The existing requirements in the EU financial services legislations and the NIS Directive would be streamlined. This will be grounded on two requirements: i) a comprehensive incident management process to monitor and log ICT incidents and ii) a mandatory reporting obligation to financial supervisors of all major ICT incidents. To enable a homogenous reporting on content and format across financial sectors, the European Supervisory Authorities would further specify the classification of ICT incidents and set uniform criteria and materiality thresholds for major ICT incidents. The initiative would require financial supervisors to pass on incident reports to the respective NIS authorities and ENISA, where relevant. In addition, new reporting obligations on ICT-related incidents in the following financial subsectors would be introduced in the EU financial services legislations: credit institutions, investment firms (except algorithmic trading), trading venues, CCPs, CSDs, trade repositories, (re)insurance, asset managers, credit rating agencies, statutory auditors. The principle of **proportionality** would apply when calibrating these provisions for the different subsectors and types of financial institutions.	Significant administrative burden reduction for those subsectors where overlapping requirements exist. Changes foreseen for those sectors where new requirements would be introduced.
Sharing of Threat Intelligence	No requirements exist in the EU financial services legislation.	The initiative will envisage introducing provisions to support/ encourage/ promote the exchange of threat intelligence among financial institutions.	Given its voluntary nature, changes might be expected for those financial institutions that would engage in such initiatives.
Digital operational resilience testing			
Advanced testing	Under the EU financial services legislation, only investment firms performing algorithmic trading are currently subject to performing more advanced testing.	More advanced testing (e.g. threat led penetration testing) would be extended to all financial subsectors and would apply only to financially significant and digitally most advanced financial institutions. The identification would be carried out using criteria laid down in the new regulation. The principle of **proportionality** would apply when calibrating these provisions for the different subsectors and types of financial institutions.	Changes might be expected for some of financial subsectors.

		New rules on the mutual acceptance of testing results performed in different Member States would be introduced.	
ICT third party risk			
Outsourcing to TPPs (indirect supervision)	The EU financial services legislation contains provisions on outsourcing to third party providers. The rules on outsourcing are diverse in scope and specificity. The following subsectors are covered by specific rules. For those not mentioned in the list, provisions are either too general or inexistent: • Credit institutions, trade repositories, asset managers, statutory auditors. The NIS Directive doesn't cover outsourcing to third party providers.	The existing requirements in the EU financial services legislations on arrangements with, including outsourcing to, ICT third party providers would be strengthened and could include provisions on e.g. rights to access, audit and obtain information from TPPs, exit strategies, notification by TPPs of the sub-outsourced services, etc. All arrangements (including outsourcing) concluded by financial institutions with ICT TPPs would contain a minimum of key contractual requirements deemed essential for a financial institution's ability to monitor ICT risks emerging at the third party. Specific rights and obligations, derived from the ESAs Guidelines on outsourcing and related supervisory practices, would apply at different stages of the contractual relationship (e.g. performance, termination and post-service assistance).	Changes might be expected for some of the financial subsectors and ICT TPPs.
Direct oversight of ICT TPPs	Under the NIS Directive, only cloud service providers (a sub-set of ICT TPPs) are currently subject to limited supervision of security requirements and incident reporting by the NIS Authority. Financial supervisors have no oversight over the activities of ICT TPPs.	ICT TPPs would become subject to a direct oversight by financial authorities. This will build upon decades of experience with oversight applied by financial supervisors to other actors and in different contexts, but innovates through an integrated EU dimension. An enhanced oversight of critical ICT TPPs will leverage on existing structures and authorities (ESAs and national supervisors, Joint Committee, colleges) with a lead EU overseer implementing a set of rights directly upon critical ICT TPPs. These would consist in e.g. access to information, audit and inspection rights, approvals or vetoes of certain operations - especially where a critical ICT TPP has no physical presence in the Union or when it envisages sub-outsourcing or where concentration of arrangements touching critical functions may trigger financial stability concerns.	Changes might be expected for both ICT TPPS and prudential supervisors.

ANNEX 5 – WHO IS AFFECTED BY THE INITIATIVE AND HOW?

1. Practical implications of the initiative

Under the retained option (**option 2: a digital operational resilience act for the financial sector**) a comprehensive framework addressing in a consistent manner at EU level the digital resilience needs of all regulated financial institutions would be established.

This EU framework would aim to strengthen the qualitative dimension of the operational risk framework by building a proper digital operational resilience core requirements (the *"core requirements"*). Under this option, *the core requirements* in the initiative would apply across the financial sector. When defining the core requirements across the four main areas, the principle of proportionality would apply both across the subsectors, but also within each subsector, taking into account, where relevant, specific needs arising for specific categories of financial institutions, as well as their business models, size, risk profile, systemic importance, etc.

Financial subsectors under the scope of the NIS Directive would remain subject to the NIS Directive and its lex specialis exemption would continue to apply to the ICT security and incident notification requirements set out in the current version of the Directive, and to any other substantive requirements that may emerge with its revision. They would therefore remain associated with the NIS 'ecosystem provisions' (national strategy, Cooperation Group, CSIRTs network, international cooperation and standardization) through a specific article in the new act and a corresponding article in the revision of the NIS Directive distinguishing between substantive and non-substantive provisions in NIS, what is applicable to financial institutions and clarifying the extent of the lex specialis. The association would materialise via, for example, the exchange of information and cooperation between financial supervisors and the NIS designated authorities or the participation of financial supervisors in the NIS Cooperation Group.

This option is broadly supported by the stakeholders responding to the public consultation (for more details see Annex 3). In particular, almost all respondents agreed that all financial entities should have in place an **ICT risk management framework** based on key common principles, with most of the respondents insisting that these common standards should be risk-based and allow for a proportionate application. In terms of basic and advanced **testing**, the majority of respondents agree that financial entities should be required to perform a baseline testing/assessment of their ICT systems and tools. Similarly, the overwhelming majority of respondents agreed that more advanced testing should be carried out for significant financial entities identified at EU level or designated by competent authorities. The majority of respondents to the public consultation agree that the EU should play a role in supporting and promoting the voluntary **information sharing** as it would help reduce information asymmetries across jurisdictions, and foster coordination, communication and cooperation among financial institutions and competent authorities. Finally, an overwhelming majority of respondents to the public consultation supported the introduction of an **oversight framework for critical ICT TPPs**.

2. Summary of cost and benefits

Benefits and costs of option 2 for each category of stakeholders have been summarized in the below table. Main benefits refer to financial institutions who would benefit from a coherent regulatory framework on digital operational resilience, increased indirect oversight over ICT

TPPS, cost savings due to streamlined reporting and reduced administrative burden on testing. The provision of financial services by more resilient financial institution would also lead to increased benefits for consumers and investors. On the supervisory side, prudential benefits would derive from an increased overview on the frequency and impact of ICT-related incidents and monitoring concentration risks from ICT TPPs. Costs would increase for all stakeholders, but to a lesser extent for consumers (e.g. if some of the cost borne by financial institutions would be passed on to their customers).

Table 9 - Impacts on different stakeholders of Option 2

	Consumers/investors	Financial institutions	ICT TPPs	Supervisors
Benefits	↑↑↑	↑↑↑	↑↑	↑↑↑
Costs	↑	↑↑	↑↑	↑↑

Tables 10 and 11 below, present the typical costs and benefits deriving from the specific actions to be undertaken for each of the main policy areas in order to implement option 2. In several instances, it is not possible to quantify impact at a high level of detail. In addition, for some policy areas in the baseline, current costs are not available/disclosed due to the sensitivity of the data. On the benefits side, most of them are of a qualitative nature. Therefore, the exercise in the following tables will accordingly follow a descriptive approach based on the benefits and costs described in detail in section 4.3.

Table 10 – Overview of benefits: preferred option

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.	*Stakeholders who benefit:* Financial institutions Supervisors

	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).	
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 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.	*Stakeholders who benefit:* Financial institutions Supervisors
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

Table 11 - Overview of costs: preferred option

		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 financial institutions' ICT systems could be passed on to their customers.	NA	NA	NA	NA	NA	NA

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 advice)	Annual costs may range between 1.000 EUR and 50.000 EUR, plus 1 to 3 FTEs.	NA	NA	NA	NA
	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	NA	NA	Adjust supervision to new rules	Marginal increase in FTEs for overseeing TLPTs and making sure it meets the requirements of the framework

					in the range of €25 to €50 million.				
	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 to monitor the activities of ICT TPPs (direct oversight)	Direct costs	NA	NA	NA	NA	Adjust to new rules of direct oversight	It is estimated that on average, the staffing costs for an ICT TPPs that would be subject to a direct oversight by financial supervisors would be in the range of 2 to 6 FTEs.	Costs for supervisory authorities participating in the different arrangements 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 participating authorities.	Higher enforcement costs
	Indirect costs	NA	NA	NA	NA	NA	NA	NA	NA

ANNEX 6 – HYPOTHETICAL SCENARIOS

The hypothetical scenarios presented in this annex are extracted from a report by the European Systemic Risk Board (ESRB)[123] and are slightly adapted based on Commission's own assessment by including some additional potential impacts and covering other financial subsectors.

The ESRB report puts forward a scenario analysis that looks deeper at how cyber risk can become a source of systemic risk to the EU financial system. The report explains why cyber risk, due to specific features, differs in significant ways from traditional revenue driven risks, such as credit, market or liquidity risks. For instance, the 2018 outages at Visa[124] and Mastercard[125] led to several hours of disruptions in the card payments market, affecting several million transactions across Europe and globally.

The ESRB assesses whether cyber risk can trigger systemic repercussions by developing a conceptual model and identifying several specific scenarios. Table 12 below presents three hypothetical scenarios to describe how a cyber incident can lead to a systemic event and how the problems addressed by this initiative are relevant to this: (1) a disruption of the ICT systems of a domestically systemic important bank; (2) a malicious destruction of account balance data of a specialised asset manager and (3) the manipulation of the price feeds of several commodities and futures markets, as well as the trade and position information that market participants receive from the market's central counterparties.

Table 12 – Hypothetical scenarios

Hypothetical scenarios	Description
Scenario 1: Incapacitation of a large domestic bank's payment system	Under this scenario, all payment functions of a domestic systemically important bank are disrupted. The bank is a significant contributor to several retail payment systems. An update generates redundant code in the IT systems of Bank X and thereby disrupts their payment software and databases. The software is purchased from and maintained by an ICT third party provider. The update of the software includes a maintenance release provided from the ICT third party provider. The disruption lasts for a long period of time, resulting in millions of transactions not being processed and financial stress and social unrest begin to materialise. The crisis is amplified by the spread of fake news on social media that Bank X has been the target of a sophisticated cyber incident. **Potential impacts:** • The bank is forced to temporarily shut down all its retail operations and this brings significant reputational business impact. • The unavailability of account balances and deposits has cascading effects and disrupts a wider range of retail services. Debit and credit card, online and mobile banking are unavailable for a while, and customers start to worry about the integrity of their accounts and losing their savings. • Fake news on social media claiming Bank X has been the target of a cyber-attack has fuelled speculation and amplified concerns by customers. This leads to a bank run, and doubts start to spread about other domestic and international banks being affected. Customers of other banks start getting anxious that their banks might experience

[123] https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf
[124] https://fintechnologynews.com/visa-admits-5-2m-payments-failed-during-the-10-hour-outage/
[125] https://www.ft.com/content/1fd2a066-860f-11e8-a29d-73e3d454535d

	similar disruptions and start withdrawing their deposits. Bank X and authorities attempt to calm the public by stating that the situation is under control. However, the inability to solve the issue quickly leads to a broader loss of public confidence in the financial system. • The ICT third party provider is servicing other domestic systemically important banks, and supervisors start inquiring about whether the update disrupted the IT systems of these banks too. • The bank in unable to open new accounts and attract new funding. Corporate clients, including small and medium sized enterprises, face revenue losses due to their inability to use their accounts. • The shares of Bank X register a sharp drop leading to loses for investors, and the bank starts facing increased risk premia in wholesale funding markets. Other domestic banks also start facing higher risk premia from international investors, due to insufficient knowledge about the market to differentiate between Bank X and other banks. **Relevance to the problems addressed by this initiative:** • The current legislation applicable to the bank (CRR/CRD) does not include specific requirements, so incident reporting, outsourcing to third party providers and testing depends on the rules imposed by the national supervisor. • In addition, the notification of the incident is made to the NIS authority, which can be different from the financial supervisor (see section 2.1.2). • On the risks stemming from the ICT third party providers, the current framework does not provide an overview to financial supervisors of which and how many financial institutions are reliant on a specific ICT third party provider, and thus supervisors lack both the awareness and the tools to address potential disruptions.
<u>Scenario 2:</u> **Malicious destruction of account balance data**	Under this scenario, cyber criminals are launching an attack on the account balance data of a specialised Asset Manager X in a Member State, which is also a market maker and has consistently under-invested in ICT systems. This leads to the loss of availability and integrity of account balances with severe impacts on both wholesale and retail clients. Under this scenario, account balances, and other data assets, are permanently destroyed. **Potential impacts:** • At first sight, only Asset Manager X is impacted. Soon after, second-order impacts (e.g. on its customers and partners) are noticed. • Asset Manager X tries to restore the data from backups and execute operations via alternative redundant platforms. However, as the malicious actors were able to alter technical recovery procedures, it becomes evident that these efforts are ineffective. By the end of the first day, customers' redemption and subscription orders are in a pending status. • Many customers did not receive confirmation of the execution of their orders. Asset Manager X's management reaches the view that there is a possibility that impacted data are lost permanently, or that recovery would at least take a considerable amount of time, possibly exceeding several weeks. Customers become concerned and there is a spike in redemption orders. Asset Manager X suffers a surge in call centre calls from customers seeking to understand the impact of the problem and wishing to establish whether their investments are safe. **Relevance to the problems addressed by this initiative:** • The specialised asset manager is not at all subject to the NIS Directive or to specific requirements on ICT risk management, incident notifications or testing under the EU financial services legislation, but could still spread panic and contagion to a full market. • Imposing key ICT risk management requirements and testing of ICT systems would have led to higher investments, and would have reduced the likelihood of the incident. • Incident reporting would have enabled authorities to timely communicate

	to the public and limit potential risks of contagion.
<u>Scenario 3:</u> **Manipulation of price and position data**	Under this scenario, cyber criminals have managed to manipulate the prices of several commodities and futures markets, as well as the trade and position information that market participants are receiving from the market's central counterparty (CCP). The threat actors have managed to insert malicious code into the ICT infrastructure used for the processing and outputting of price, trade and position data. This leads to a situation of uncertainty around the reliability of prices and positions, and consequently traders are pulling out of the market causing liquidity to drop, prices to drop sharply and automatic stop losses to be triggered. The resultant market panic takes on a self-reinforcing and self-sustaining dynamic, which causes severe losses for multiple market participants across several market segments. Under this scenario, severe market disruption including the default of certain trading firms, and potentially the affected central counterparties materialises. **Potential impacts:** • Market data providers and a central counterparty are simultaneously targeted in the incident. The affected market participants begin doubting the accuracy of reported prices and positions. As they continue to worry about the reliability and accuracy of prices, some traders begin exiting positions. • As more and more market participants become unwilling to trade, market liquidity falls, adding further doubts regarding the state of the market. Due to the drop in liquidity and traders seeking to exit positions, volatility increases and prices continue to fall. • Automatic stop losses are triggered. These are generating a new wave of sell orders across multiple market segments, which further increases price drops and volatility spikes, and feeds negatively into the confidence channel. **Relevance to the problems addressed by this initiative:** • The CCP is subject to EMIR rules and thus supervised by the financial supervisor with regards to its ICT risk management arrangements and needs to report the incident to the financial supervisor. • At the same time, the CCP may be subject to the NIS Directive if identified as operator of essential services, and thus may be required to report the incident separately to the NIS authority, which can be different from the financial supervisor. • In terms of testing, if the CCP has a cross-border presence, it may be subject to testing under different frameworks in several Member States.

Source: ESRB, Commission's own assessment.

While the ESRB report acknowledges that to date no cyber incidents with systemic impact for the financial system have materialised, it is nevertheless important to highlight that some elements of these hypothetical scenarios have already materialized:

- For instance, the incident at Bank of Valetta obliged the bank to temporarily suspend all operations to minimize risk and review its systems. The bank resumed operations the next day, while payments to third parties remained unavailable over a week since the breach impacted the system that processed such payments.[126]
- In 2014 in Bulgaria, a spam newsletter distributed via email and social media caused bank runs at two major national banks, with depositors withdrawing the equivalent of 10% and 20% of the total assets held by these banks.[127]

[126] https://timesofmalta.com/articles/view/bov-payments-to-third-parties-remain-unavailable-after-cyber-attack.702732
[127] https://www.bruegel.org/2014/07/fact-of-the-week-a-spam-newsletter-caused-a-bank-run-in-bulgaria

- Another example is the Carbanak and Cobalt attack, where cyber criminals infiltrated over 100 financial institutions in 40 countries (including several EU countries) resulting in cumulative losses of over €1 billion for the financial industry. Cyber criminals were able in this case to increase the amount of money in a bank customer's account and then steal the 'made-up funds'.[128]
- A report by Group-IB points out to an incident at a trading terminal owned by a bank where cyber criminals perpetrated into the systems and artificially manipulated a currency pair quotes on the forex market by executing trades, which temporarily distorted the quotes. The attack lasted only a few minutes during which trades of around $250 million were executed.[129]

Such scenarios may appear extreme at first sight, but they are very plausible and the ESRB report highlights that "*disruptive cyber incidents seem to be a question of **when** rather than **if***".

[128] https://www.forbes.com/sites/thomasbrewster/2015/02/16/staples-hackers-made-one-billion-dollars/#1451caa037d0 and https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain.
[129] https://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf

ANNEX 7 – GLOSSARY

Capital buffer	A mandatory capital that financial institutions are required to hold. Capital buffers were mandated for banks under the Basel III regulatory reforms, which were implemented following the 2007-2008 financial crisis. Source: Adapted from Basel III.
CCPs	Central clearing counterparty, a legal person that interposes itself between the counterparties to the contracts traded on one or more financial markets, becoming the buyer to every seller and the seller to every buyer. Source: EMIR, Regulation (EU) No 648/2012 on OTC derivatives, central counterparties and trade repositories.
CERTs	Computer Emergency Response Teams, teams of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle. Source: Adapted from NIS, Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.
CIO	Chief Information Officer
CIP	Directive 2008/114/EC on the identification and designation of European critical infrastructures and assessment of the need to improve their protection.
CISO	Chief Information Security Officer
Concentration risk	Exposure(s) that may arise within or across different risk categories throughout an institution with the potential to produce: (i) losses large enough to threaten the institution's health or ability to maintain its core operations; or (ii) a material change in an institution's risk profile.
CRD IV	Capital Requirements Directive IV, Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms.
CRAR	Credit Rating Agencies Regulation (EU) No 462/2013.
CSDR	Regulation (EU) No 909/2014 on improving securities settlement in the European Union and on central securities depositories.
CSIRTs	Computer Security Incident Response Teams Source: NIS, Directive 2016/1148 concerning measures for a high common level of security of network and information systems

	across the Union.
Cyber-attack	An attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. Source: Adapted from Merriam-Webster
Cyber incident	A cyber event that jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or it violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. Source: FSB Lexicon
Digital operational resilience	Digital operational resilience is a broad concept, and it refers to the qualitative processes that a financial institution undergoes to build, maintain and review, on a continuous basis, its full operational integrity, for a safe and compliant running of its operations and deployment of services. That requires the activation of a set of comprehensive functions, policies, processes that allow the financial institution to be prepared to protect its ICT systems and prevent disruptions, to adapt to changing ICT patterns and to recover from those disruptions (within certain limits of tolerance either acceptable or known in advance). Digital operational resilience requirements thus address both the institution's internal organisation processes and its inherent technological dependencies to third parties for the deployment of ICT supporting business functions – in particular in relation to the monitoring of the digital risks posed by third parties through outsourcing arrangements.
eIDAS	Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market.
EMIR	European Market Infrastructure Regulation, Regulation (EU) No 648/2012 on OTC derivatives, central counterparties and trade repositories.
ENISA	European Network and Information Security Agency
ESAs	European Supervisory Authorities, composed of the EBA (European Banking Authority), ESMA (European Securities Markets Authority) and EIOPA (European Insurance and Occupational Pensions Authority).
ESRB	European Systemic Risk Board

EU stress tests	The assessment at EU level of the impact of certain developments, including macro- or microeconomic scenarios, on the overall capital and liquidity positions of selected institutions, including on their minimum or additional own funds requirements, by means of projecting the institutions' capital resources and requirements, highlighting the institutions' vulnerabilities and assessing their capacity to absorb losses and the impact on their solvency and liquidity positions. Source: Adapted from the EBA Guidelines on institutions' stress testing, EBA/GL/2018/04
Exchange of information	The act passing relevant information from one competent authority to another competent authority, done in the spirit of cooperation.
FMIs	Financial market infrastructures are critically important financial institutions responsible for providing clearing, settlement and recording of monetary and other financial transactions.
FSB	Financial Stability Board
FTE	Full-time employee
GDPR	General Data Protection Regulation, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
ICT	Information and Communication Technology
ICT risks	Risks arising with the use of network and information systems or communication technology. That includes malfunctions, hardware and software failures, disruptions caused by human error, spam, viruses etc., misuses or other types of adverse malicious and non-malicious events that can compromise the security and resilience of such network information systems or communications technologies, or the operation and running of processes or the provision of services. For example, major losses are incurred when data or ICT systems lose integrity or become unavailable, confidential data is breached or physical ICT infrastructures are damaged.
ICT risk management	ICT risk management is used to describe the application of risk management processes and mechanisms to information and communication technologies in order to manage operational risk of a digital nature. It is a component of the wider operational risk management system of any business that makes use of ICT solutions. Every firm, in the financial sector and outside, should identify risks to its ICT systems and data in order to reduce or manage those risks and develop a response plan in the event of a crisis.

IMF	International Monetary Fund
Incident reporting	Notification of financial institutions to the competent authority of a major operational or security event having an actual adverse effect on the security of network and information systems. Source: Adapted from NIS, Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union and PSD2, Directive (EU) 2015/2366 on payment services in the internal market.
Information sharing	An exchange of data, information and/or knowledge between financial institutions, which can be used to manage risks or respond to events. Source: Adapted from FSB Lexicon.
IORPS	Institutions for Occupational Retirement Directive, Directive (EU) 2016/2341 on the activities and supervision of institutions for occupational retirement provision.
ISO	International Organization for Standardization
Large exposure	In the banking context, the sum of all exposures of a bank to a single counterparty that are equal to or above 10% of its Tier 1 capital. Source: Adapted from BCBS.
Lex specialis	"Lex specialis derogate legi generali." Special law repeals general laws. A principle according to which a rule of *lex specialis* is deemed to apply notwithstanding contrary general principles of international law. The priority given to *lex specialis* is considered justified by the fact that the *lex specialis* is intended to apply in specific circumstances regardless of the rules applicable more generally where those circumstances may be absent. Source: Oxford Reference.
MiFID	Markets in financial instruments directive, Directive 2014/65/EU on markets in financial instruments.
NIS	Network and Information Systems Directive, Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.
OES	A public or private entity designated as an "operator of essential services" under NIS, Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

Oversight	A supervisory framework that monitors and addresses the security, operational reliability, business continuity, risk identification, technology planning, communication with users and overall digital operational resilience of ICT third party providers' activities and services. Source: Adapted from Swift.
PSD2	Payment Services Directive, Directive (EU) 2015/2366 on payment services in the internal market.
Systemic risk	A risk of disruption in the financial system with the potential to have serious negative consequences for the financial system and the real economy. Source: CRD IV, Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms.
Single Rulebook	A harmonised set of prudential rules, dealing inter alia with capital requirements for banks, protection for depositors, prevention and management of bank failures, that EU financial institutions must abide to. Source: Adapted from the website of the Council of the European Union, https://www.consilium.europa.eu/en/policies/banking-union/single-rulebook/.
Solvency II	Directive 2009/138/EC on the taking-up and pursuit of the business of insurance and reinsurance.
SRB	Single Resolution Board
SSM	Single Supervisory Mechanism. It refers to the system of financial supervision composed by the ECB and the national supervisory authorities of the participating Member States. Source: Council Regulation (EU) No 1024/2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions
Target2	The real-time gross settlement system owned and operated by the Eurosystem. Central banks and commercial banks can submit payment orders in euro to TARGET2, where they are processed and settled in central bank money, i.e. money held in an account with a central bank. TARGET2 settles payments related to the Eurosystem's monetary policy operations, as well as bank-to-bank and commercial transactions. Source: ECB website

	https://www.ecb.europa.eu/paym/target/target2/html/index.en.html.
Testing	A set of information security reviews and assessments performed by financial institutions to ensure the effective identification of vulnerabilities and to validate the robustness and effectiveness of their ICT systems and ICT services. It comprises gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews, source code reviews, vulnerability assessments, penetration tests and red team exercises. Source: Adapted from the EBA Guidelines on ICT and security risk management, EBA/GL/2019/04.
Threat-Led Penetration Testing	A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations. In some jurisdictions this may be referred as Ethical Red Teaming. Source: G7 Fundamentals for TLPT.
Threat intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Source: FSB Lexicon.
TIBER-EU	The European framework for Threat Intelligence-Based Ethical Red-Teaming developed by the ECB.
TPPs	Third party providers are organizations that have entered into business relationships or contracts with financial entities to provide an ICT product or service. One important type of third party relationship is outsourcing, whereby a third party provides a business function, service or process that would otherwise be provided by the financial institutions itself. TPPs include, for example, data providers and cloud services providers. Source: Adapted from the G7 Cyber Expert Group "Fundamental Elements for Third Party cybersecurity risk management in the financial sector".
Trade repository	A legal person that centrally collects and maintains the records of derivatives. Source: EMIR, Regulation (EU) No 648/2012 on OTC derivatives, central counterparties and trade repositories
Vulnerability	Systematic examination of an information system, and its

Assessment	controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. Source: FSB Lexicon.