EUROPEAN COMMISSION
Directorate-General for Financial Stability, Financial Services and Capital Markets Union

CONSULTATION DOCUMENT

Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure

Disclaimer

This document is a working document of the Commission services for consultation and does not prejudge the final decision that the Commission may take.

The views reflected on this consultation paper provide an indication on the approach the Commission services may take but do not constitute a final policy position or a formal proposal by the European Commission.

The responses to this consultation paper will provide important guidance to the Commission when preparing, if considered appropriate, a formal Commission proposal.

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
https://ec.europa.eu/info/business-economy-euro_en

You are invited to reply **by 19 March 2020** at the latest to the **online questionnaire** available on the following webpage:
https://ec.europa.eu/info/publications/finance-consultations-2019-financial-services-digital-resilience_en

Please note that in order to ensure a fair and transparent consultation process **only responses received through the online questionnaire will be taken into account and included in the report summarising the responses**.

This consultation follows the normal rules of the European Commission for public consultations. Responses will be published unless respondents indicate otherwise in the online questionnaire.

Responses authorised for publication will be published on the following webpage: https://ec.europa.eu/info/publications/finance-consultations-2019-financial-services-digital-resilience_en

CONTENT OF THE CONSULTATION DOCUMENT

Public consultation on a potential initiative on the digital operational resilience in the area of financial services

Introduction

Digitalisation and new technologies are significantly transforming the European financial system and the way it provides financial services to Europe's businesses and citizens. Almost two years after the Commission adopted the Fintech Action Plan in 2018, the actions set out in it have largely been implemented.

In order to promote digital finance in Europe while adequately regulating its risks, and in light of the mission letter of Executive Vice President Dombrovskis, the Commission services are working towards a new Digital Finance Strategy for the EU. Key areas of reflection include deepening the Single Market for digital financial services, promoting a data-driven financial sector in the EU while addressing its risks and ensuring a true level playing field, making the EU financial services regulatory framework more innovation-friendly, and enhancing the digital operational resilience[1] of the financial system.

This public consultation, and the public consultation on crypto assets published in parallel, are first steps towards potential initiatives which the Commission is considering in that context. The Commission may consult further on other issues in this area in the coming months.

The financial sector is the largest user of information and communications technology (ICT) in the world, accounting for about a fifth of all ICT expenditure[2]. Its operational resilience hinges to a large extent on ICT. This dependence will further increase with the growing use of emerging models, concepts or technologies, as evidenced by financial services benefitting from the use of distributed ledger and artificial intelligence. At the same time, an increased use of artificial intelligence in financial services may generate a need for stronger operational resilience and accordingly for ensuring an appropriate supervision. Accordingly, whether we talk about online banking or insurance services, mobile payment applications, digital trading platforms, high frequency trading algorithms, digital clearing and settlement systems, financial services delivered today rely on digital technologies and data.

Dependence on ICT and data raises new challenges in terms of operational resilience. The increasing level of digitalisation of financial services coupled with the presence of high value assets and (often sensitive) data make the financial system vulnerable to operational incidents and cyber-attacks. While it already outspends other sectors in safeguarding itself against ICT risks (both of malicious and accidental nature) finance is nonetheless estimated to be three times more at risk of cyber-attacks than any other sector[3]. In the recent years, the frequency and impact of cyber incidents has been increasing, with research estimating the total cost in the range of tens to

1 Without the intention to provide a definition, the concept of "digital operational resilience" is used throughout the document to refer to the ability of a financial entity to build and maintain its operational integrity and the full range of operational capabilities, related to any digital and data technology-dependant component, tool, process that the financial entity uses to conduct and support its business. It encompasses ICT and security risk management.

2 According to Statista, 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.

3 European Parliament report on "Fintech: the influence of technology on the future of the financial sector" (2016/2243(INI)) http://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.pdf

hundreds of billions of Euro for the global economy. The increasing digitalisation of finance is set to accelerate this trend. The ever-increasing number and sophistication of cyber-threats and ICT incidents in the financial sector illustrate the importance and urgency to tackle the incidence and effects of these risks in a pre-emptive way. Operational resilience issues, and in particular ICT and security risks can also be source of systemic risk for the financial sector. These issues should be addressed as an integral part of the EU regulatory framework and single rulebook that aims to ensure the competitiveness, integrity, security and stability of the EU financial sector.

The EU financial sector is governed by a detailed and harmonised single rulebook, ensuring proper regulation and a level playing field across the single market, which in some areas forms the basis for EU bodies to supervise specific financial institutions (e.g. Single Supervisory Mechanism supervision of credit institutions). The EU financial services regulatory landscape already includes certain ICT and security risk provisions and, more generally, operational risk provisions, but these rules are fragmented in terms of scope, granularity and specificity. ICT and security risks are one of the major components of operational risk, which prudential supervisors should assess and monitor as part of their mandate. In order to preserve and build a harmonised approach and implement international standards in the financial sector with a view to more effectively address digital operational resilience issues and to raise trust and stimulate digital innovation, it is essential that financial supervisors' efforts work in a harmonised and convergent framework across Member States and across different parts of the financial sector. Where EU bodies have direct supervisory responsibilities over certain financial institutions, this will also ensure that they have the necessary and appropriately framed powers.

The EU has taken steps towards a horizontal cyber security framework that provides a baseline across sectors.[4] The ICT and security risks faced by the financial sector and its level of preparedness and integration at EU level warrant specific and more advanced co-ordinated actions that build on, but go substantially beyond the horizontal EU cyber security framework and that are commensurate with a higher degree of digital operational resilience and cyber security maturity expected from the financial sector.

Under its Fintech Action Plan,[5] the European Commission asked the European Supervisory Authorities (i.e. the European Banking Authority, the European Securities and Markets Authority, and European Insurance and Occupational Pensions, hereinafter the "ESAs") to map the existing supervisory practices across financial sectors around ICT security and governance requirements, to consider issuing guidelines aimed at supervisory convergence and, if necessary provide the Commission with technical advice on the need for legislative improvements. The Commission also invited the ESAs to evaluate the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector.

Building on that, the focus of this public consultation is to inform the Commission on the development of a potential EU cross-sectoral digital operational resilience framework in the area of financial services. This consultation aims 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.

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

[5] FinTech Action plan: For a more competitive and innovative European financial sector, COM/2018/0109 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109

Stakeholders mapping

The following relevant stakeholder groups have been identified:

- Public authorities: Member States governments, national competent authorities, all relevant actors of the financial supervisory community including at EU level (EU supervisory authorities and other relevant EU agencies or bodies).

- Industry, business associations, SMEs: financial services providers (e.g. credit institutions, (re)insurance companies, investment firms, central counterparties, central securities depositories, trade repositories, credit rating agencies, audit firms, asset managers, regulated markets, payment service providers etc.), ICT services providers.

- Consumers, financial services and ICT services users, civil society.

- Academia and public interest organisations and think tanks

Context of the present consultation

There is broad political agreement at international level that cyber risks in the financial sector must be addressed by enhancing and reviewing cyber resilience. Cyber resilience as part of the broader work on the operational resilience of financial institutions is a priority for many financial supervisors and regulators across the globe, with several ongoing work streams in various international fora (i.e. G7, FSB, BCBS, CPMI-IOSCO).

At EU level, the European Parliament called on the Commission "to make cybersecurity the number one priority" in taking the work forward in its FinTech Action Plan.[6] It also emphasised the need for more supervisory oversight into cyber risks, more cooperation among competent authorities, as well better information sharing among market participants regarding cyber threats, and more investment into effective cyber-defences.

The Commission's Fintech Action Plan has set out plans to develop a dedicated approach to cyber security which is a part of the operational resilience for the EU financial sector. A dedicated approach to enhance what can be referred to as the digital operational resilience of financial institutions is even more relevant in the context of the increase in outsourcing arrangements and third party dependencies (e.g. through cloud adoption). As committed in the Fintech Action Plan, the Commission has responded with several policy actions, among which the upcoming development of Standard Contractual Clauses for cloud arrangements with financial sector entities. Further to that, and with an eye to future legislative improvements, the ESAs published a joint Technical Advice in April 2019.[7] Their assessment demonstrated the existence of fragmentation in the scope, granularity and specificity of ICT and security/ cyber security provisions across the EU financial services legislation. The ESAs hence called on the Commission to propose legislative changes in the area of ICT and cyber security for the EU financial sector, allowing the identified gaps and inconsistencies to be addressed.

More specifically, they propose legislative changes in four main areas: (1) requirements on ICT and security risk management in the legislative acquis applicable to the financial sector, (2) streamlining the existing incident reporting requirements (3) setting out a cyber resilience testing

[6] European Parliament report on "Fintech: the influence of technology on the future of the financial sector" (2016/2243(INI)), http://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.pdf

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

framework and (4) establishing an oversight of ICT third party providers to the financial institutions.

More recently, in the informal ECOFIN discussion in September 2019 on the resilience of financial institutions against cyber and “hybrid” threats, Member States also highlighted the urgent need for having in place better testing, more information sharing and enhanced coordination between authorities.[8]

In this context, the Commission is launching a public consultation to explore how an enhanced framework for digital operational resilience of the EU financial sector could be set up. This goal could be achieved through an EU cross-sectoral initiative for the financial sector that would take into account the strengths and specificities of existing international, EU and national frameworks and developments on ICT security and risk management.

For more information or additional questions please contact:

fisma-digital-operational-resilience@ec.europa.eu

[8] See https://eu2019.fi/documents/11707387/15400298/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf/29565728-f476-cbdd-4c5f-7e0ec970c6c4/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf

----

PART I

1. STAKEHOLDER IDENTIFICATION, TRANSPARENCY AND CONFIDENTIALITY

PART II

2. BUILDING BLOCKS FOR A POTENTIAL EU INITIATIVE: MAIN ISSUES

Although a horizontal EU cyber security framework are in place across various sectors[9], ICT and security risk in the area of financial services has so far only been partially addressed in the EU regulatory and supervisory framework. This framework has traditionally focussed on propping up the financial resilience of various institutions by means of additional capital and liquidity buffers and regulating their conduct in order to protect their users and clients. Less focus has gone into operational stability and in particular into building digital operational resilience. This includes risks related to the growing digitalisation of finance, outsourcing and the consequent need for greater cyber-vigilance. The horizontal EU cyber security framework does not fully reflect the increasingly important role that ICT plays in the financial sector, and the risks it can pose to the operational resilience of an institution, consumer trust and confidence, and, by extension, to financial stability.

Following up on the advice submitted by the three ESAs in April 2019, the Commission is seeking stakeholders' views in the areas of:

- **Targeted improvements of ICT and security risk management requirements** across the different pieces of EU financial services legislation. Such improvements are needed to reinforce the level of digital operational resilience across all main financial sectors subject to the EU financial regulatory framework. They could build on existing requirements in EU law, taking into account standards, guidelines or recommendations on operational resilience, which have already been agreed internationally (e.g. guidelines issued by the ESAs, G7, Basel Committee, CPMI-IOSCO).[10]
- **Harmonisation of ICT incidents reporting**: rules on reporting should be clarified and complemented with provisions facilitating a better monitoring and analysis of ICT and security-related risks. This exercise could look into setting out what qualifies as a reportable incident and setting materiality thresholds in this respect, setting out relevant time frames, while also clarifying reporting lines and harmonising templates to bring further consistence and ease of use.
- The **development of a digital operational resilience testing framework** across all financial sectors, providing for a mechanism to anticipate threats and improve the digital operational readiness of financial actors and authorities. This assessment could look into setting key requirements to perform digital operational resilience testing while

[9] NIS Directive and Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (The EU Cybersecurity Act).

[10] For instance, EBA Guidelines on ICT and security risk management, EBA Guidelines on outsourcing arrangements, G-7 Fundamental Elements of Cybersecurity for the Financial Sector, G-7 Fundamental Elements for Threat-Led Penetration Testing, G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector, BCBS Cyber-resilience: range of practices, CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, etc.

maintaining flexibility and proportionality to address specific needs of financial actors by virtue of their size, complexity and scale of operations.

- Specific rules enabling a **better oversight of certain critical ICT third-party providers** which regulated financial institutions rely on, and outsource functions to.
- Specific arrangements **to promote** a) **effective information sharing** on ICT and security threats among financial market participants and b) **better cooperation** among public authorities.

2.1. ICT and security requirements

In their Joint Advice, the three ESAs point to different, sometimes inconsistent terminology across the financial services acquis. In addition, when it comes to ICT and security risk,[11] the EU financial services acquis appears fragmented in the level of detail and specificity of such provisions. Currently, rules on ICT and security risk (sometimes implicitly considered under operational risk requirements, other times explicitly referred to in terms of ICT-requirements) seem patchy. Some regulated financial entities are subject to more specific requirements (e.g. under PSD2, CSDR, EMIR, etc.)[12], while for other financial entities such rules are rather general or even inexistent (e.g. CRD/CRR, Solvency II, UCITS/AIFMD, etc.)[13]. Not all EU legislation addresses the full spectre of ICT and security risk management requirements based on standards, guidelines or recommendations on cyber risk management and operational resilience agreed internationally (e.g. G7, Basel Committee, CPMI-IOSCO, etc.). Further, requirements are not uniformly spread out between Level 1 (Regulations, Directives) and Level 2 (delegated and implementing acts) texts across the different financial sectors.

The three ESAs note overall an absence of explicit provisions on ICT and security risk management. They plead for clarity about a minimum level of ICT security and governance requirements. On this basis, a set of improvements related to ICT-risk management requirements may be needed to reinforce the cybersecurity readiness and resilience across all key financial sectors.

__Questions:__

1. *Taking into account the deep interconnectedness of the financial sector, its extensive reliance on ICT systems and the level of trust needed among financial actors, do you agree that all financial entities should have in place an ICT and security risk management framework based on key common principles?*

   - ☐ *Yes*
   - ☐ *No*
   - ☐ *Don't know/no opinion*

---

[11] The EBA has recently published its Guidelines on ICT and security risk management (EBA/GL/2019/04) applicable to all institutions under the EBA remit and aim to strengthen institutions' resilience against ICT and security risks. https://eba.europa.eu/eba-publishes-guidelines-ict-and-security-risk-management

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

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

To the extent you deem it necessary, please explain your reasoning.

2. *Where in the context of the risk management cycle has your organisation until now faced most difficulties, gaps and flaws in relation to its ICT resilience and preparedness? Please rate each proposal from 1 to 5, 1 standing for 'not problematic' and 5 for 'highly problematic').*

Stage in the risk management cycle (or any other relevant related element)	*1*	*2*	*3*	*4*	*5*	*Don't know/not applicable*
Identification						
Detection						
Ability to protect						
Respond						
Recovery						
Learning and evolving						
Information sharing with other financial actors on threat intelligence						
Internal coordination (within the organisation)						
Other (please specify)						

To the extent you deem it necessary, please explain your reasoning.

3. *What level of involvement and/or what type of support/ measure has the Board (or more generally the senior management within your organisation) offered or put in place/provided for, in order to allow the relevant ICT teams to effectively manage the ICT and security risk? Please rate each proposal from 1 to 5, 1 standing for 'no support/ no measure' and 5 for 'high support/very comprehensive measures').*

Type of involvement, support or measure	*1*	*2*	*3*	*4*	*5*	*Don't know/not applicable*
Appropriate allocation of human and financial resources						
Appropriate investment policy in relation to the ICT and security risks						
Approval by the Board of an ICT strategy (that also deals with ICT security aspects)						
Active role of the Board (or the senior management) when your organisation faces major cyber incidents or, as the case may be, role of the Board in the ICT business continuity policy						

Top leadership and guidance received in relation to ICT security and ICT risks						
Other (please specify)						

To the extent you deem it necessary, please explain your reasoning and emphasize in addition any type of support and measure that you consider that you consider the Board and senior management should provide.

4. *How is the ICT risk management function implemented in your organisation?*

   To the extent you deem it necessary, please explain your reasoning.

5. *Which main arrangements, policies or measures you have in place to identify and detect ICT risks?*

Type of arrangement, policy, measure	*Yes*	*No*	*Don't know/not applicable*
Do you establish and maintain an updated mapping of your organisation's business functions, roles and supporting processes?			
Do you have an up-to-date registry/inventory of supporting ICT assets (e.g. ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes)?			
Do you classify the identified business functions, supporting processes and information assets based on their criticality?			
Do you map all access rights and credentials and do you use a strict role-based access policy?			
Do you conduct a risk assessment before deploying new ICT technologies / models?			
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

6. *Have you experienced cyber-attacks with serious repercussions for your clients or counterparties?*

   - ☐ *Yes*
   - ☐ *No*
   - ☐ *Don't know/Not applicable*

To the extent you deem it necessary, please explain and illustrate in particular the nature of the attack and the impacts on the clients/counterparts.

7. *How many cyber-attacks does your organisation face on average every year? How many of these have/are likely to create disruptions of the critical operations or services of your organisation?*

   Please explain your reasoning.

8. *Do you consider that your ICT systems and tools are appropriate, regularly updated, tested and reviewed to withstand cyber-attacks or ICT disruptions and to assure their operational resilience? Which difference do you observe in this regard between in-house and outsourced ICT systems and tools?*

   - *Yes*
   - *No*
   - *Don't know/Not applicable*

   To the extent you deem it necessary, please explain your reasoning.

9. *Has your organisation developed and established a cloud strategy?*

   - *Yes*
   - *No*
   - *Don't know/no opinion*

10. *If the answer to the previous question (no. 9) is yes, please explain which of the following aspects are covered and how.*

	Yes	*No*	*Don't know/not applicable*
Do you use on-premise cloud technology?			
Do you use off-premise cloud technology			
Does this strategy contribute to managing and mitigating ICT risks?			
Do you use multiple cloud service infrastructure providers? How many?			
Did your Board and senior management establish a competence center for cloud in your organisation?			

   To the extent you deem it necessary, please explain your reasoning.

11. *Do you have legacy ICT systems that you would need to reconsider for enhanced ICT security requirements? What would be the level of investments needed (in relative or absolute terms)?*

   - *Yes*
   - *No*
   - *Don't know/Not applicable*

To the extent you deem it necessary, please explain your reasoning.

12. *What in your view are possible causes of difficulties you experienced in a cyber-attack/ ICT operational resilience incident? Please rate each answer from 1 to 5, 1 standing for 'not problematic' and 5 for 'highly problematic').*

Causes of difficulties	*1*	*2*	*3*	*4*	*5*	*Don't know/not applicable*
ICT environmental complexity						
Issues with legacy systems						
Lack of analysis tools						
Lack of skilled staff						
Other (please specify)						

To the extent you deem it necessary, please explain your reasoning.

13. *Do you consider that your organisation has implemented high standards of encryption?*

- ☐ *Yes*
- ☐ *No*
- ☐ *Don't know/Not Applicable*

To the extent you deem it necessary, please explain your reasoning.

14. *Do you have a structured policy for ICT change management and regular patching and a detailed backup policy?*

- ☐ *Yes*
- ☐ *No*
- ☐ *Don't know/not Applicable*

To the extent you deem it necessary, please explain your reasoning.

15. *Do you consider that your organisation has established and implemented security measures to manage and mitigate ICT and security 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)?*

- ☐ *Yes*
- ☐ *No*
- ☐ *Don't know/Not applicable*

To the extent you deem it necessary, please explain your reasoning and for which measures legal clarity and simplification would be needed.

16. *On average, how quickly do you restore systems after ICT incidents, in particular after a serious/major cyber-attack? Are there any differences in that respect based on where the impact was (impact on the availability, confidentiality or rather the integrity of data)?*

    To the extent you deem it necessary, please specify and explain.

17. *Which issues you struggle most with, when trying to ensure a quick restoration of systems and the need to maintain continuity in the delivery of your (critical) business functions?*

Issues	*Yes*	*No*	*Don't know/not applicable*
Lack of comprehensive business continuity policy and/or recovery plans			
Difficulties to keep critical/ core business operations running and avoid shutting down completely			
Internal coordination issues (i.e. within your organisation) in the effective deployment of business continuity and recovery measures			
Lack of common contingency, response, resumption/recovery plans for cyber security scenarios - when more financial actors in your particular ecosystem are impacted			
No ex-ante determination of the precise required capacities allowing the continuous availability of the system			
Difficulties of the response teams to effectively engage with all relevant (i.e. business lines) teams in your organization to perform any needed mitigation and recovery actions			
Difficulty to isolate and disable affected information systems			
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

18. *What are your views on having in the legislation a specific duration for the Recovery Time Objective (RTO) and having references to a Recovery Point Objective (RPO)?*

    To the extent you deem it necessary, please explain your reasoning.

19. *Through which activities or measures do you incorporate lessons post-incidents and how do you enhance the cyber security awareness within your organisation?*

	Yes	*No*	*Don't know/not*

			applicable
Do you promote staff education on ICT and security risk through regular information sessions and/or trainings for employees?			
Do you regularly organize dedicated trainings for the Board members and senior management?			
Do you receive from the Board all the support you need for implementing effective cyber incident response and recovery improvement programs?			
Do you make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents? Do you conduct ex post root cause analysis of cybersecurity incidents?			
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

2.2. ICT and security incident reporting requirements

The ESAs advise the Commission to consider a comprehensive, harmonised system of ICT incident reporting requirements for the financial sector. This should be designed to enable financial entities to report accurate and timely information to competent authorities, in order to allow firms and authorities to properly log, monitor, analyse and adequately respond to ICT and security risks and mitigate fraud. The ESAs propose that templates, taxonomy and timeframes should be standardised where possible. Finally, the relationship with existing incident reporting requirements, e.g. under the Payment Services Directive (PSD2) or Central Securities Depositories Regulation (CSDR), as well as under the NIS Directive and GDPR, should be clarified.

Questions:

20. *Is your organisation currently subject to ICT and security incident reporting requirements?*

- ☐ *Yes*
- ☐ *No*
- ☐ *Don't know/Not applicable*

To the extent you deem it necessary, please explain your reasoning.

21. *Do you agree that a comprehensive and harmonised EU-wide system of ICT and security incident reporting should be designed for all financial entities?*

- ☐ *Yes*
- ☐ *No*
- ☐ *Don't know*

To the extent you deem it necessary, please explain your reasoning.

22. *If the answer to the previous question (no. 21) is yes, please explain which of the following elements should be harmonised?*

Elements to be harmonised in the EU-wide system of ICT incident reporting	*Yes*	*No*	*Don't know/not applicable*
Taxonomy of reportable incidents			
Reporting templates			
Reporting timeframe			
Materiality thresholds			
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

23. *What level of detail would be required for the ICT and security incident reporting? Please elaborate on the information you find useful to report on, and what may be considered as unnecessary.*

    To the extent you deem it necessary, please explain your reasoning.

24. *Should all incidents be within the scope of reporting, or should materiality thresholds be considered, whereby minor incidents would have to be logged and addressed by the entity but still remain unreported to the competent authority?*

    - ☐ *Yes*
    - ☐ *No*
    - ☐ *Don't know*

    To the extent you deem it necessary, please explain your reasoning.

25. *Which governance elements around ICT and security incident reporting would be needed? To which national competent authorities should ICT and security incidents be reported or should there be one single authority acting as an EU central hub/database?*

    To the extent you deem it necessary, please explain your reasoning.

26. *Should a standing mechanism to exchange incident reports among national competent authorities be set up?*

    - ☐ *Yes*
    - ☐ *No*
    - ☐ *Don't know*

    To the extent you deem it necessary, please explain your reasoning.

27. *What factors or requirements may currently hinder cross-border cooperation and information exchange on ICT and security incidents?*

    To the extent you deem it necessary, please explain your reasoning and provide concrete examples.

2.3. Digital operational resilience testing framework

Financial institutions must regularly assess the effectiveness of their preventive, detection and response capabilities to uncover and address potential vulnerabilities. The ESAs advice identifies several tools to achieve this objective and recommends implementing a *multi-stage gradual approach* that sets a common denominator amongst all financial entities and raises the bar of the digital operational resilience across the EU financial sector. In the short term, ESAs recommend to focus on prevention, ensuring that entities perform the basic assessment of their cyber vulnerabilities. In the medium-longer term, the ESAs suggest developing a coherent *cyber resilience testing framework* across the EU financial sectors, together with setting-up of a common set of guidance that could lead to the mutual acceptance/recognition of the test results across the EU supervisory community.

In general, a digital resilience testing[14] can be a highly effective tool to uncover aspects of ICT and security policy that are lacking, to provide real-life feedback on some routes most at risk into the entity's systems and networks, as well as to raise awareness on ICT security and resilience within the financial entity. It can also facilitate the creation of a single market for intelligence and test providers.

If different EU regulatory driven testing frameworks emerge across Member States, financial entities are potentially faced with increased costs and duplication of work. Facilitation, synchronisation and EU-wide cooperation would thus be advisable.

Questions:

28. *Is your organisation currently subject to any ICT and security testing requirements?*

- ☐ *Yes*
- ☐ *No*
- ☐ *Don't know/not applicable*

If the answer is yes:

	Yes	*No*	*Don't know/ not applicable*
Do you face any issues with overlapping or diverging obligations?			
Do you practice ICT and security testing on a voluntary basis?			

To the extent you deem it necessary, please explain your reasoning.

29. *Should all financial entities be required to perform a baseline testing/assessment of their ICT systems and tools? What could its different elements be?*

Different elements of a baseline testing/assessment framework	*Yes*	*No*	*Don't know/ not applicable*

[14] Without the intention to provide a definition, the concept of "digital operational resilience testing" refers throughout the document to techniques, tools and measures to assess the effectiveness of a financial entity's preventive, detection, response and recovery capabilities to uncover and address potential vulnerabilities. It includes both a baseline testing/assessment (e.g. gap analysis, vulnerability scans, etc.) and more advanced testing (e.g. threat led penetration testing, TLPT).

Gap analyses?			
Compliance reviews?			
Vulnerability scans?			
Physical security reviews?			
Source code reviews?			
Others (please specify)			

To the extent you deem it necessary, please explain your reasoning.

30. *For the purpose of being subject to more advanced testing (e.g. threat led penetration testing, TLPT), should financial entities be identified at EU level (or should they be designated by competent authorities) as "significant" on the basis of a combination of criteria such as:*

Criteria	*Yes*	*No*	*Don't know/ not applicable*
Proportionality–related factors (i.e. size, type, profile, business model)?			
Impact – related factor (criticality of services provided)?			
Financial stability concerns (Systemic importance for the EU)?			
Other appropriate qualitative or quantitative criteria and thresholds (please specify)?			

To the extent you deem it necessary, please explain your reasoning.

31. *In case of more advanced testing (e.g. TLPT), should the following apply?*

	Yes	*No*	*Don't know/ not applicable*
Should it be run on all functions?			
Should it be focused on live production systems?			
To deal with the issue of concentration of expertise in case of testing experts, should financial entities employ their own (internal) experts that are operationally independent in respect of the tested functions?			
Should testers be certified, based on recognised international standards?			
Should tests run outside the Union be recognised as equivalent if using the same parameters (and thus be			

held valid for EU regulatory purposes)?			
Should there be one testing framework applicable across the Union? Would TIBER-EU be a good model?			
Should the ESAs be directly involved in developing a harmonised testing framework (e.g. by issuing guidelines, ensuring coordination)? Do you see a role for other EU bodies such as the ECB/SSM, ENISA or ESRB?			
Should more advanced testing (e.g. threat led penetration testing) be compulsory?			

To the extent you deem it necessary, please explain your reasoning.

32. *What would be the most efficient frequency of running such more advanced testing given their time and resource implications?*

- *Every six months*
- *Every year*
- *Once every three years*
- *Other*

To the extent you deem it necessary, please explain your reasoning.

33. *The updates that financial entities make based on the results of the digital operational testing can act as a catalyst for more cyber resilience and thus contribute to overall financial stability. Which of the following elements could have a prudential impact?*

	Yes	*No*	*Don't know/ not applicable*
The baseline testing/assessment tools (see question 29)?			
More advanced testing (e.g. TLPT)?			
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

2.4. Addressing third party risk: Oversight of third party providers (including outsourcing)

Financial entities use third party ICT service providers to outsource a large number of their activities. While this brings significant opportunities, it may also create new risks for financial entities and specifically may relocate existing operational, ICT, security, governance and reputational risks to third party technology providers. Furthermore, it can lead to legal and compliance issues, to name just a few, that can originate at the third party or derive from ICT and security vulnerabilities within the third party.

A set of general principles should be available in the legal framework to orient different financial institutions in their set-up and management of contractual arrangements with third party providers, also enabling a better overview of risks stemming from third parties and any subsequent chain of outsourcing.

The widespread use of ICT third party providers can also lead to concentration risk in the availability of ICT third party providers, their substitutability and in the portability of data between them. This can impair financial stability. Some ICT third party providers are globally active, so concentration risks - together with other risks such as location of data - further increase. That is even more so in the current context of regulatory fragmentation.

The ESAs recommend establishing an appropriate third party oversight framework to address the need of a better monitoring of such risks posed by ICT third party providers. The framework should set out criteria for identifying the critical nature of the ICT third party providers, define the extent of the activities that are subject to the framework and designate the authority responsible to carry out the oversight.

Questions:

34. *What are the most prominent categories of ICT third party providers which your organisation uses?*

    To the extent you deem it necessary, please explain your reasoning.

35. *Have you experienced difficulties during contractual negotiations between your organisation and any ICT third party providers, specifically with regard to establishing arrangements reflecting the outsourcing requirements of supervisory/regulatory authorities?*

    - ☐ *Yes*
    - ☐ *No*
    - ☐ *Don't know/not applicable*

    To the extent you deem it necessary, please explain your reasoning, elaborating on which specific outsourcing requirements were difficult to get reflected in the contract(s).

36. *As part of the Commission's work on Standard Contractual Clauses for cloud arrangements with financial sector entities, which outsourcing requirements best lend themselves for standardisation in voluntary contract clauses between financial entities and ICT third party service providers (e.g. cloud)?*

    To the extent you deem it necessary, please explain your reasoning

37. *What is your view on the possibility to introduce an oversight framework for ICT third party providers?*

	Yes	*No*	*Don't know/not applicable*
Should an oversight framework be established?			
Should it focus on critical ICT third party providers?			
Should "criticality" be based on a set of both qualitative and quantitative thresholds (e.g. concentration, number of customers, size, interconnectedness, substitutability, complexity,			

etc.)?			
Should proportionality play a role in the identification of critical ICT third party providers?			
Should other related aspects (e.g. data portability, exit strategies and related market practices, fair contractual practices, environmental performance, etc.) be included in the oversight framework?			
Should EU and national competent authorities responsible for the prudential or organisational supervision of financial entities carry out the oversight?			
Should a collaboration mechanism be established (e.g. within colleges of supervisors where one national competent authority assumes the lead in overseeing a relevant ICT service provider to an entity under its supervision - see e.g. CRD model)?			
Should the oversight tools be limited to non-binding tools (e.g. recommendations, cross-border cooperation via joint inspections and exchanges of information, onsite reviews, etc.)?			
Should it also include binding tools (such as sanctions or other enforcement actions)?			

To the extent you deem it necessary, please explain your reasoning.

38. *What solutions do you consider most appropriate and effective to address concentration risk among ICT third party service providers?*

	Yes	*No*	*Don't know/not applicable*
Diversification strategies, including a potential mandatory or voluntary rotation mechanism with associated rules to ensure portability (e.g. auditing model)			
Mandatory multi-provider approach			
Should limits be set by the legislator or supervisors to tackle the excessive exposure of a financial institution to one or more ICT third party providers?			

Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

2.5. Other areas where EU Action may be needed

<u>Information sharing:</u> This part tackles information sharing needs of different financial entities - something distinct from either reporting (which takes place between the financial entities and the competent authorities) or cooperation (among competent authorities).

Information sharing contributes to the prevention of cyber-attacks and the spreading of ICT threats. Exchanges of information between the financial institutions - such as exchange on tactics, techniques and procedures (TTPs) and indicators of compromise (IOCs) - help ensure a safe and reliable ICT environment which is paramount for the functioning of the integrated and interconnected financial sector.

<u>Questions:</u>

39. *Do you agree that the EU should have a role in supporting and promoting the voluntary exchanges of such information between financial institutions?*

    - ☐ *Yes*
    - ☐ *No*
    - ☐ *Don't know/no opinion*

    To the extent you deem it necessary, please explain your reasoning.

40. *Is your organisation currently part of such information-sharing arrangements?*

    - ☐ *Yes*
    - ☐ *No*
    - ☐ *Don't know/no opinion*

    To the extent you deem it necessary, please explain your reasoning. If you have answered yes to the question, please explain how these arrangements are organised and with which financial counterparts you exchange this information. Please specify the type of information exchanged and the frequency of exchange.

41. *Do you see any particular challenges associated with the sharing of information on cyber threats and incidents with your peer financial institutions?*

    - ☐ *Yes*
    - ☐ *No*
    - ☐ *Don't know/no opinion*

    To the extent you deem it necessary, please explain your reasoning. If you answered yes, please explain which are the challenges and why, by giving concrete examples.

42. *Do you consider you need more information sharing across different jurisdictions within the EU?*

    - ☐ *Yes*
    - ☐ *No*

- *Don't know/no opinion*

To the extent you deem it necessary, please explain your reasoning and clarify which type of information is needed and why its sharing is beneficial.

<u>Promotion of cyber insurance and other risk transfer schemes:</u> In an increasingly digitalized financial sector facing an important number of cyber incidents, there is a need for financial institutions and their supervisors to better understand the role that insurance coverage for cyber risks can play. Both the demand and supply sides of the market in Europe for cyber insurance and for other risk transfer instruments should be further analysed.

<u>Questions:</u>

43. *Does your organisation currently have a form of cyber insurance or risk transfer policy?*

    - *Yes*
    - *No*
    - *Don't know/no opinion*

    If you answered yes, please specify which form of cyber insurance and whether it comes as a stand-alone cyber risk insurance policy or is offered bundled with other more traditional insurance products.

44. *What types of cyber insurance or risk transfer products would your organisation buy or see a need for?*

    To the extent you deem it necessary, please specify and explain whether they should cover rather first or third-party liability or a combination of both?

45. *Where do you see challenges in the development of an EU cyber insurance/risk transfer market, if any?*

Issues	*Yes*	*No*	*Don't know/not applicable*
Lack of a common taxonomy on cyber incidents			
Lack of available data on cyber incidents			
Lack of awareness on the importance of cyber/ICT security			
Difficulties in estimating pricing or risk exposures			
Legal uncertainties around the contractual terms and coverage			
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning, by also specifying to the extent possible how such issues or lacks could be addressed.

46. *Should the EU provide any kind of support to develop EU or national initiatives to promote developments in this area? If so, please provide examples.*

- *Yes*
- *No*
- *Don't know/no opinion*

To the extent you deem it necessary, please explain your reasoning.

2.6. Interaction with the NIS Directive

The NIS Directive is the first internal market horizontal instrument aimed at improving the resilience of the EU against cybersecurity risks across different critical sectors[1] by ensuring a minimum level of harmonisation.

As far as financial services are concerned, entities from three sectors fall in the scope of the Directive: credit institutions, operators of trading venues and central counterparties. Entities from other financial services sectors (for instance insurance and reinsurance undertakings, trade repositories, central securities depositories, data reporting services providers, asset managers, investment firms, credit rating agencies etc.) are not in the scope of the NIS Directive. Their relevant ICT and security risk requirements remain covered by other specific pieces of legislation.

The lex specialis clause of the NIS Directive allows for the application of sector-specific EU legislation when such legislation has requirements in relation to the security of network and information systems or the notification of incidents that are at least equivalent to the NIS Directive requirements[15].

With regard to the entities belonging to the critical sectors referred to in Annex II of the NIS Directive, the co-legislators have given broad room for discretion to Member States when identifying which particular entities in these critical sectors should be under the scope of the Directive. In particular, the Member States are required to carry out the identification of ‘operators of essential services’ based on three criteria spelled out in the NIS Directive.

<u>Questions:</u>

47. *Does your organisation fall under the scope of application of the NIS Directive (i.e. is identified as operator of essential services) as transposed in your Member State?*

- *Yes*
- *No*
- *Don't know/no opinion*

To the extent you deem it necessary, please explain your situation in this respect. If you answered yes to the question, please specify the requirements you are subject to, indicating the financial sector you are operating in.

48. *How would you asses the effects of the NIS Directive for your specific financial organisation? How would you assess the impact of the NIS Directive on your financial sector - taking into account the 3 specific financial sectors in its scope (credit institutions,*

---

15 Article 1(7) of the NIS Directive (“Where sector-specific … requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply”.)

trading venues and central clearing parties), the designation of operators of essential services and the lex specialis clause?

To the extent you deem it necessary, please explain your reasoning.

49. *Are you covered by more specific requirements as compared to the NIS Directive requirements and if so, do they originate from EU level financial services legislation or do they come from national law?*

    To the extent you deem it necessary, please explain your reasoning and provide details.

[For **financial institutions** established in a Member State that has designated as NIS competent authority a national authority that is not a financial supervisor]:

50. *Did you encounter issues based on the fact that in the Member State where you are established the NIS competent authority is not the same as your own financial supervisory authority?*

    Please provide details on your experience in the context of the application of NIS and explain any issues you may have encountered.

51. *How do you cooperate with the NIS competent authority in the Member State where you are established? Do you have agreements for cooperation/MoUs?*

    Please provide details on your experience.

[For **financial supervisors, designated NIS competent authorities, single points of contact**]

52. *Do you receive NIS relevant information in relation to a financial entity under your remit?*

    Please detail your experience, specifying how this information is shared (e.g. ad hoc, upon request, regularly) and providing any information that may be disclosed and you consider to be relevant.

53. *Would you see merit in establishing at EU level a rule confirming that the supervision of relevant ICT and security risk requirements - which a regulated financial institution needs to comply with - should be entrusted with the relevant European and national financial supervisor (i.e. prudential, market conduct, other etc.)?*

    Please explain your reasoning

54. *Did you encounter any issue in getting access to relevant information, the reporting of which originates from the NIS requirements (i.e. incident reporting by a financial entity under your remit/supervision)?*

    - ☐ *Yes*
    - ☐ *No*
    - ☐ *Don't know/no opinion*

    If you answered yes, please explain those particular issues.

55. *Have you encountered any issues in matters involving cross-border coordination?*

    - ☐ *Yes*
    - ☐ *No*
    - ☐ *Don't know/no opinion*

If you answered yes, please explain which issues.

56. *What is your experience with the concrete application of the lex specialis clause in NIS?*

    Please explain by providing, whenever possible, concrete cases where you either found the application of the lex specialis helpful, or otherwise where you encountered difficulties or faced doubts with the application or interpretation of specific requirements and the triggering of the lex specialis.

3. POTENTIAL IMPACTS

The initiative is likely to create a more secure digital environment in the operation and use of complex ICT tools and processes underpinning the provision of financial services. It is expected that such increase in the overall digital operational resilience of the financial institutions (which encompasses ICT and security risk) would not only benefit the overall financial stability but also result in higher level of consumer protection and enable innovative data driven business models in finance.

Questions:

57. *To the extent possible and based on the information provided for in the different building blocks above, which possible impacts and effects (i.e. economic, social, corporate, business development perspective etc.) could you foresee, both in the short and the long term?*

    Please provide details.

58. *Which of the specific measures set out in the building blocks (as detailed above) would bring most benefit and value for your specific organisation and your financial sector? Do you also have an estimation of benefits and the one-off and/or recurring costs of these specific measures?*

    Please provide details.

59. *Which of these specific measures would be completely new for your organisation and potentially require more steps/gradual approach in their implementation?*

    Please provide details.

60. *Where exactly do you expect your company to put most efforts in order to comply with future enhanced ICT risk management measures and with increased safeguards in the digital environment? For instance, in respect to your current ICT security baseline, do you foresee a focus on investing more in upgrading technologies, introducing a corporate discipline, ensuring compliance with new provisions such as testing requirements, etc.?*

    Please provide details.

61. *Which administrative formalities or requirements in respect to the ICT risks are today the most burdensome, human-resource intensive or cost-inefficient from an economic perspective? And how would you suggest they should be addressed?*

    Please provide details.

62. *Do you have an estimation of the costs (immediate and subsequent) that your company incurred because of ICT incidents and in particular cyber-attacks? If yes, to the extent possible, please provide any useful information (in relative or absolute) terms that you may disclose.*

    Please provide details.