Contribution ID: 896ddc82-2e7f-437e-8f4e-62ef2bc9b0ac
Date: 17/03/2020 13:25:38

Public consultation on a digital operational resilience framework for financial services: making the EU financial sector more resilient and secure

Fields marked with * are mandatory.

Introduction

This consultation is also available in German and French.

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 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. European Central Bank/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, 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.

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[5]. 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. 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 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.

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.

---

[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))

[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] European Parliament report on "Fintech: the influence of technology on the future of the financial sector" (2016/2243(INI))

Please note: In order to ensure a fair and transparent consultation process **only responses received through our online questionnaire will be taken into account** and included in the report summarising the responses. Should you have a problem completing this questionnaire or if you require particular assistance, please contact fisma-digital-operational-resilience@ec.europa.eu.

More information:

- on this consultation
- on the consultation document
- on the protection of personal data regime for this consultation

1. About you

* Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- (•) English
- Estonian
- Finnish
- French
- Gaelic
- German
- Greek
- Hungarian
- Italian
- Latvian
- Lithuanian
- Maltese
- Polish
- Portuguese

- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as

- Academic/research institution
- Business association
- Company/business organisation
- Consumer organisation
- EU citizen
- Environmental organisation
- Non-EU citizen
- Non-governmental organisation (NGO)
- Public authority
- Trade union
- Other

* First name

Jan Wolfgang

* Surname

Doser

* Email (this won't be published)

jan.wolfgang.doser@deutsche-boerse.com

* Organisation name

255 character(s) maximum

Deutsche Börse Group

* Organisation size

- Micro (1 to 9 employees)
- Small (10 to 49 employees)
- Medium (50 to 249 employees)
- Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

20884001341-42

* Country of origin

Please add your country of origin, or that of your organisation.

- Afghanistan
- Åland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Djibouti
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar /Burma
- Namibia
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden

- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam

- Cuba
- Curaçao
- Cyprus
- Czechia
- Democratic Republic of the Congo
- Denmark
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- Saint Lucia
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia
- Zimbabwe

* Field of activity or sector (if applicable):

at least 1 choice(s)

- [ ] Accounting
- [ ] Auditing
- [ ] Banking
- [ ] Investment firm
- [ ] Payment service provider
- [ ] Credit rating agencies
- [ ] Insurance
- [ ] Pension provision
- [ ] Investment management (e.g. hedge funds, private equity funds, venture capital funds, money market funds, securities)
- [x] Market infrastructure operation (e.g. CCPs, CSDs, Stock exchanges)
- [ ] Social entrepreneurship
- [ ] Cybersecurity expert
- [ ] Academia
- [ ] Business organisations/associations
- [ ] Other
- [ ] Not applicable

* Publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

- **Anonymous**
  Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.
- **Public**
  Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

☑ I agree with the personal data protection provisions

2. Building blocks for a potential EU initiative: main issues

Although a horizontal EU cyber security framework are in place across various sectors[6], 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)[7].
- **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 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.

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

[7] 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.

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[8], 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.)[9], while for other financial entities such rules are rather general or even inexistent (e.g. CRD/CRR, Solvency II, UCITS/AIFMD, etc.)[10]. 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.

[8] 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

[9] 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.

[10] 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.

Question 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 / not relevant

Question 1.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 1:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

From our point of view, if an actor relies on ICT systems, it has to have ICT and security risk management frameworks in place. This is not limited to the financial industry only. Useful ISO standards already exist, which can be applied (e.g. 27001 and 27005).

Question 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 from 1 (not problematic) to 5 (highly problematic)

	1 (not problematic)	2	3	4	5 (highly problematic)	Don't know / no opinion / not relevant
Identification	○	○	○	○	○	○
Detection	○	◉	○	○	○	○
Ability to protect	○	○	◉	○	○	○
Respond	○	○	○	◉	○	○
Recovery	○	○	○	○	○	○
Learning and evolving	○	○	○	◉	○	○
Information sharing with other financial actors on threat intelligence	○	○	○	◉	○	○
Internal coordination (within the organisation)	○	○	○	○	○	○

Question 2.1 Is there any other stage in the risk management cycle (or any other relevant related element) in which your organisation until now faced most difficulties, gaps and flaws? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 2.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 2:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As Deutsche Börse Group (DBG) consists of different entities, offering different services and using various ICT systems, it is not possible to give generalized answers in every dimension of those kind of questions. Due to the fact that our response will be publicly available, we do not answer some questions intentionally.

Question 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 from 1 (no support/no measure) to 5 (high support/very comprehensive measures)

	1 (no support/ no measure)	2	3	4	5 (high support/ very comprehensive measures)	Don't know / no opinion / not relevant
Identification	○	○	○	○	○	○
Detection	○	○	○	○	○	○
Ability to protect	○	○	○	○	○	○
Respond	○	○	○	○	○	○
Recovery	○	○	○	○	○	○
Learning and evolving	○	○	○	○	○	○

Information sharing with other financial actors on threat intelligence						
Internal coordination (within the organisation)						

Question 3.1 Any other type of involvement, support or measure? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 3.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 3 and emphasise in addition any type of support and measure that you consider that you consider the Board and senior management should provide:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 4. How is the ICT risk management function implemented in your organisation?
To the extent you deem it necessary, please explain your reasoning.

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As already stated above, DBG consists of different entities, nonetheless risks are identified and tracked centrally with support of decentralized application teams.

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

	Yes	No	Don't know / no opinion / not relevant
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?	○	○	○

Question 5.1 Any other type of arrangement, policy, measure? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 5.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 5:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

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

- ○ Yes
- ◉ No
- ○ Don’t know / no opinion / not relevant

Question 6.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 6:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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.

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

See Question 6.

Question 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 / no opinion / not relevant

Question 8.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 8:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

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

- (●) Yes
- ( ) No
- ( ) Don’t know / no opinion / not relevant

Question 9.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 9:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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 / no opinion / not relevant
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?	◉	○	○

Question 10.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 10:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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 / no opinion / not relevant

Question 11.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 11:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 12. What in your view are possible causes of difficulties you experienced in a cyber-attack/ ICT operational resilience incident?

Please rate from 1 (not problematic) to 5 (highly problematic)

	1 (not problematic)	2	3	4	5 (highly problematic)	Don't know / no opinion / not relevant
ICT environmental complexity	○	○	○	○	○	◉
Issues with legacy systems	○	○	○	○	○	◉
Lack of analysis tools	○	○	○	○	○	◉
Lack of skilled staff	○	○	○	○	○	◉

Question 12.1 Is there any other possible causes of difficulties you experienced in a cyber-attack/ ICT operational resilience incident? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 12.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 12:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

See Question 6.

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

- ○ Yes
- ○ No
- ◉ Don’t know / no opinion / not relevant

Question 13.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 13:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

DBG is currently implementing higher standards with regard to encryption than before.

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

- ◉ Yes
- ○ No
- ○ Don’t know / no opinion / not relevant

Question 14.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 14:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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 / no opinion / not relevant

Question 15.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 15 and for which measures legal clarity and simplification would be needed:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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.

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

See Question 6.

Question 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?

	Yes	No	Don't know / no opinion / not relevant
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 organisation to perform any needed mitigation and recovery actions	○	○	◉
Difficulty to isolate and disable affected information systems	○	○	○

Question 17.1 Is there any other issue you struggle with, when trying to ensure a quick restoration of systems and the need to maintain continuity in the delivery of your (critical) business functions? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 17.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 17:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

See Question 6.

Question 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 specify and explain.

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As Deutsche Börse Group consists of different entities offering different services and using various ICT systems, we are aware of the complexity in the financial industry. Hence, we think that the definition of such rules on a general level and in an adequate manner would be difficult to achieve. Therefore, we would recommend that legislation could define non-binding RTO and RPO durations as general guidelines and only foresee requirements to uphold the functionality within specific contexts. Nonetheless, if a cross-sectoral framework for digital operational resilience would be considered on the EU level, the specifics should be aligned with other regulatory requirements for the financial sector (e.g. MiFID II / MiFIR, EMIR and associated technical standards), which also contain operational resilience requirements.

Question 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 / no opinion / not relevant
Do you promote staff education on ICT and security risk through regular information sessions and/or trainings for employees?	◉	○	○
Do you regularly organise 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?	○	○	○

Question 19.1 Is there any other activity or measures through which you incorporate lessons post-incidents, or ways to enhance the cyber security awareness within your organisation? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 19.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 19:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

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.

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

- (●) Yes
- ( ) No
- ( ) Don't know / no opinion / not relevant

Question 20.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 20:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As already indicated, due to the specific structure within DBG, the security incident reporting requirements are depending on the specific entity and the services offered.
Relevant requirements can be found for example in
- Art. 23 (3) (EU) Commission Delegated Regulation 2017/584 (relevant for trading venues);
- Art. 45 (6) 2 (EU) Regulation 909/2014 (relevant for central securities depositories);
- Art. 75 (9) (EU) Commission Delegated Regulation 2017/392 (relevant for central securities depositories);
- Art.7 and 9 (4) (EU) Commission Delegated Regulation 2017/571 (relevant for data reporting service providers);
- § 8b (4) BSI Act in connection with § 7 (1) 1. KRITIS ordinance;
- Art. 33 (1) GDPR

As a general remark, it would be preferable if future rules could be more detailed, would incorporate common standards and share the same taxonomy.

Question 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 / no opinion / not relevant

Question 21.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 21:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We would support such a system, if it would make ICT and security incidents more comparable and would help to identify issues, gaps and flaws. At the same time, it should be ensured that a comprehensive and harmonised EU-wide system of ICT and security incident reporting reflects the specific requirements of the different areas of the financial industry covered, to be proportionate.

Question 22. If the answer to question 21) is yes, please explain which of the following elements should be harmonised?

	Yes	No	Don't know / no opinion / not relevant
Taxonomy of reportable incidents	◉	○	○
Reporting templates	◉	○	○
Reporting timeframe	◉	○	○
Materiality thresholds	◉	○	○

Question 22.1 Is there any other element that should be harmonised in the EU-wide system of ICT incident reporting? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 22.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 22:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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 specify and explain.

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As there will be a range of types of entities that will be covered by respective legislation, the level of details regarding ICT and security incident reporting should be rather low.

Question 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 / no opinion / not relevant

Question 24.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 24:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

From a security perspective, it would be beneficial to report as much incidents as possible to enclose their potential effects. However, we do not think that all incidents should be within the scope of reporting, as it could be unproportionally burdensome for the reporting entities to report any incident in a complete and harmonized manner. Thus, without carefully designed materiality thresholds, the provision of reports would become disproportionate.

Question 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 specify and explain.

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We think that it would make sense in terms of subsidiarity, clarity, quality of the data collection and knowledge as well as experience to share the responsibilities between the NCAs and a central hub /database. NCAs could collect the information and ensure the data quality by pre-checking the information, before handling them over to the central database, which would then further process and analyse the data and share the results respectively.

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

- (●) Yes
- ( ) No
- ( ) Don't know / no opinion / not relevant

Question 26.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 26:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

If a central EU hub would be created to analyze the information collected by the NCAs, it would be beneficial to share the results among them (see answer to Q25).

Question 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 specify and explain.

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

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 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.

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

- (●) Yes
- ( ) No
- ( ) Don’t know / no opinion / not relevant

Question 28.1 Do you face any issues with overlapping or diverging obligations?

- ( ) Yes
- ( ) No
- ( ) Don’t know / no opinion / not relevant

Question 28.2 Do you practice ICT and security testing on a voluntary basis?

- ( ) Yes
- (●) No
- ( ) Don’t know / no opinion / not relevant

Question 28.3 To the extent you deem it necessary, please explain your reasoning for your answers to question 28 (and possible sub-questions):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

With regard to our "application security concept", security testing and penetration testing are required to be documented.

Question 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?

	Yes	No	Don't know / no opinion / not relevant
Gap analyses?	◉	○	○
Compliance reviews?	◉	○	○
Vulnerability scans?	◉	○	○
Physical security reviews?	◉	○	○
Source code reviews?	◉	○	○

Question 29.1 Is there any other element of a baseline testing/assessment framework that all financial entities should be required to perform? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We think that penetration testing would be necessary, as this can uncover additional vulnerabilities, that have not been considered before.

Question 29.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 29:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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:

	Yes	No	Don't know / no opinion / not relevant
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)?	◉	○	○

Question 30.1 Are there any other appropriate qualitative or quantitative criteria and thresholds? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 30.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 30:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

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

	Yes	No	Don't know / no opinion / not relevant
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?	◉	○	○

Question 31.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 31:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We think it would be beneficial if more advanced testing would focus on live production systems, but also test systems could be considered.

Question 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

Question 32.1 To the extent you deem it necessary, please explain your reasoning for your answer to question 32:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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 / no opinion / not relevant
The baseline testing/assessment tools (see question 29)?	(●)	( )	( )
More advanced testing (e.g. TLPT)?	(●)	( )	( )

Question 33.1 Is there any other element that could have a prudential impact? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 33.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 33:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

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.

Question 34. What are the most prominent categories of ICT third party providers which your organisation uses? To the extent you deem it necessary, please specify and explain.

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Deutsche Börse Group uses various ICT third party providers along its value chain, which are offering a variety of services (e.g. providers of data center, cloud service providers, providers of traditional soft and hardware). Therefore, a prioritization is not possible.

Question 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 / no opinion / not relevant

Question 35.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 35, elaborating on which specific outsourcing requirements were difficult to get reflected in the contract(s):

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Cloud Service Providers (CSP) offer their highly standardized scalable services to many different clients. Hence, they generally not cater for individual specifics of industries Thus requirements of the financial industry often need CSP verification with CSP inhouse stakeholders. Some requirements of financial institutions are not readily implemented. The contractual requirements thus often do not reflect these requirements and need individual negotiation.

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.
Experienced difficulties: unrestricted audit rights for regulators, customer and its external auditors subcontracting information and control rights to CSP customer's benefit, information rights, instruction rights, recovery time objectives, post-termination assistance, resolution requirements under BRRD directive, extension of the required rights along outsourcing chains to regulated end-customers.

Question 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 specify and explain.

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We think that voluntary contract clauses, which would address the issues mentioned in Q35, could be highly beneficial and appreciated by the financial industry. If they would be designed in a reasonable way, those clauses could act as the starting point of future negotiations between financial institutions and ICT third party service providers, especially CSPs. Good examples are the Standard Contractual Clauses (SCC) for data transfer between EU and non-EU countries in the area of data protection.

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

	Yes	No	Don't know / no opinion / not relevant
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)?	○	○	○

Question 37.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 37:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

If a EU framework is considered, the principles of subsidiarity and proportionality should be respected.

The here presented criteria defining “criticality” are rather vague (concentration, number of customers…). Further details would be needed to assess any oversight framework properly.

A new strict oversight framework on EU level, covering all ICT third party providers would be complex and could harm the competitiveness of EU financial institutions, as it could make the outsourcing of services of financial institutions to ICT service providers more difficult.

Question 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 / no opinion / not relevant
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?	○	◉	○

Question 38.1 Is there any other solution that you would consider most appropriate and effective to address concentration risk among ICT third party service providers? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As of today, the European ICT industry is not yet as developed as in other countries, which is not only true for cloud- and software-, but as well as for hardware-services. Therefore, we think that only competition and an innovation friendly regulatory environment could be effective in the long-term, to reduce the concentration risks.

Question 38.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 38:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We oppose the mandatory solutions mentioned above, as they would most likely be very expensive or/and ineffective, as they are not addressing the core problem of the situation (see Q38.1).

2.5. Other areas where EU Action may be needed

Information sharing: 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.

Question 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 / not relevant

Question 39.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 39:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

There already existing fora (e.g. the WFE Global Exchange Cyber Security Working Group) which could be promoted to foster the voluntary exchange of information.

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

- (●) Yes
- ( ) No
- ( ) Don't know / no opinion / not relevant

If you answered yes to question 40, 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:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 40.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 40 (and its possible sub-question):

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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 / not relevant

If you answered yes to question 41, please explain which are the challenges and why, by giving concrete examples:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 41.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 41 (and its possible sub-question):

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

When information about cyber threats and incidents are getting shared, information about the IT systems in use also have to be disclosed. This may have implications with regard to competitiveness of a company due to the potential disclosure of business secrets.

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

- Yes
- No
- Don’t know / no opinion / not relevant

Question 42.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 42 and clarify which type of information is needed and why its sharing is beneficial:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Promotion of cyber insurance and other risk transfer schemes: In an increasingly digitalised 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.

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

- (•) Yes
- No
- Don’t know / no opinion / not relevant

If you answered yes to question 43, 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:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 43.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 43 (and its possible sub-question):

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The organisation has an insurance policy for cyber risks in place. The policy is a stand-alone cyber risk insurance policy.

Question 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:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A cyber insurance policy should provide cover, in the event, that claims for compensation of a financial loss are made against the insured by other parties, due to a breach of information security and on the basis of legal liability provisions under private law. Further, it should provide insurance cover if, due to information security breach the business of the insured is interrupted or impaired. Additionally, costs and expenses (mainly crisis management and forensic) related to a cyber attack should be carried by such an insurance policy.

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

			Don’t know /

	Yes	No	no opinion / not relevant
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	◉	○	○

Question 45.1 Is there any other area for which you would see challenges in the development of an EU cyber insurance/risk transfer market? Please specify which one(s) and explain your reasoning:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 45.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 45, by also specifying to the extent possible how such issues or lacks could be addressed:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 46. Should the EU provide any kind of support to develop EU or national initiatives to promote developments in this area?

- ◉ Yes
- ○ No
- ○ Don’t know / no opinion / not relevant

If you think the EU provide any kind of support to develop EU or national initiatives to promote developments in this area, please explain your reasoning and provide examples:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 46.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 46 (and possible sub-questions):

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Yes, the companies need more awareness of the cyber risks and safety. The EU should provide statistics and a better documentation of attacks.

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 (see Annex II of the Directive) 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[11].

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.

[11] 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".)

Question 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 / not relevant

If you answered yes to question 47, please specify the requirements you are subject to, indicating the financial sector you are operating in:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 47.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 47 (and its possible sub-question):

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As stated above, Deutsche Börse Group consists of different entities, therefore only some parts fall under the NIS Directive.

Question 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, 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:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 49. Are you covered by more specific requirements as coplease explain your reasoning mpared 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:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Yes, see Question 20.

Special question: in order to select the next questions that will be asked to you, please specify if you are:

- a financial institution established in a Member State that has designated as NIS competent authority a national authority that is not a financial supervisor
- a financial supervisor, designated NIS competent authorities, single points of contact
- none of these

Questions 50 and 51 are specific questions addressed to financial institutions established in a Member State that has designated as NIS competent authority a national authority that is not a financial supervisor.

Questions from 52 to 56 are specific questions addressed to financial supervisors, designated NIS competent authorities, single points of contact.

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.

Question 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 explain your reasoning and provide details:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We share the perspective, that the initiative would contribute to the overall financial stability. However, additional regulatory requirements would increase the internal efforts of a company to be compliant. Therefore, new obligations should be aligned with existing rules and should also be attainable as efficiently as possible.

Question 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 explain your reasoning and provide details:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We think that it would be most beneficial to establish specific arrangements to promote effective information sharing on ICT and security threats among financial market participants and to facilitate better cooperation among public authorities (see the last of the mentioned building blocks).

Question 59. Which of these specific measures would be completely new for your organisation and potentially require more steps/gradual approach in their implementation? Please explain your reasoning and provide details:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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 explain your reasoning and provide details:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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 explain your reasoning and provide details:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 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?

- Yes
- No
- Don't know / no opinion / not relevant

Question 62.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 62 (and its possible sub-question):

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Additional information

Should you wish to provide additional information (e.g. a position paper, report) or raise specific points not covered by the questionnaire, you can upload your additional document(s) here:

The maximum file size is 1 MB.
You can upload several files.
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

Useful links

More on the Transparency register (http://ec.europa.eu/transparencyregister/public/homePage.do?locale=en)

More on this consultation (https://ec.europa.eu/info/publications/finance-consultations-2019-financial-services-digital-resilience_en)

Specific privacy statement (https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement_en)

Consultation document (https://ec.europa.eu/info/files/2019-financial-services-digital-resilience-consultation-document_en)

Contact

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