FESE response to the Commission consultation on Digital Operational Resilience Framework for financial services

Brussels 18th March

Q1 - 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

Q1.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 1:

FESE welcomes the possibility to respond to the European Commission consultation on digital operational resilience framework for financial services. Exchanges play an important role in promoting the stability of the financial system and are taking several measures to ensure their cyber resilience. This is also already subject to supervision by competent authorities. While there is a need for a coordinated approach on the subject, it is important that flexibility to innovation is safeguarded and ‘one-size-fits-all’-procedures are not put in place. In considering potentially further developing regulatory requirements in this space, it should be kept in mind that there is often more than one way of addressing an issue without necessarily compromising the result and by limiting modes of action, vulnerability could, as an unintended consequence, be built into the system.

FESE would caution against overly prescriptive measures and advocate for solutions that ensure the necessary flexibility to meet the individual needs of exchanges, the markets they service, and the challenges/threats they all face. Moreover, any requirement to disclose details on cyber resilience should be conducted in a careful manner to ensure sharing of such information does not unintentionally better equip potential attackers, thereby increasing cyber resilience-related risk. A potential approach should be sufficiently broad to encompass multiple cyber risks and avoid recommending specific, overly prescriptive, and quantitative parameters.

The Commission indicates that it would intend to build a potential enhanced framework on “the strengths and specificities of existing international, EU and national frameworks and developments on ICT security and risk management.” We consider this very important to avoid re-inventing the wheel and continue allowing best practices. It should be noted that there are a number of industry-led initiatives and solutions that work through experience sharing, cooperating and collaborating with industry groups, examples include WFE Global Exchange (GLEX) Cyber Security Working Group.

Any proposed security risk management framework should be based in internationally developed standards. We believe that NIST Cybersecurity Framework (CSF) in recent years has become the de facto standard of choice in the financial sector adopted by a majority of financial entities. Furthermore, it has gained wide-spread adoption by governments and financial regulators across many jurisdictions. CPMI-IOSCO Guidance on Cyber resilience for FMIs, ECB's Cyber Resilience Oversight Expectations for FMI and G7 Fundamental Elements of Cybersecurity for the Financial Sector are entirely based on NIST CSF.

Q2 - 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)						

Q2.1 - 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:

N/A

Q2.2 - To the extent you deem it necessary, please explain your reasoning for your answers to question 2:

N/A

Q3 - 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*
Identification						
Detection						
Ability to protect						
Respond						
Recovery						
Learning and evolving						
Information sharing with other financial actors on threat intelligence						
Internal coordination (within the organisation)						

Q3.1 - Any other type of involvement, support or measure? Please specify which one(s) and explain your reasoning:

N/A

Q3.2 - 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:

N/A

Q4 - How is the ICT risk management function implemented in your organisation?

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

N/A

Q5 - 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 updated a 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?			

Q5.1 - Any other type of arrangement, policy, measure?

Please specify which one(s) and explain your reasoning:

N/A

Q5.2 - To the extent you deem it necessary, please explain your reasoning for your answers to question 5:

N/A

Q6 - Have you experienced cyber-attacks with serious repercussions for your clients or counterparties?

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

Q6.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 6:

N/A

Q7 - 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.

N/A

Q8 - 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

Q8.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 9:

N/A

Q9 - Has your organisation developed and established a cloud strategy?

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

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

N/A

Q10 - 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 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?			

Q10.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 10:

N/A

Q11 - 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

Q11.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 11:

N/A

Q12 - 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						

Q12.1 - 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:

N/A

Q12.2 - To the extent you deem it necessary, please explain your reasoning for your answers to question 12:

N/A

Q13 - Do you consider that your organisation has implemented high standards of encryption?

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

Q13.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 13:

N/A

Q14 - 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

Q14.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 14:

N/A

Q15 - 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

Q15.1 - To the extent you deem it necessary, please explain your reasoning and for which measures legal clarity and simplification would be needed:

N/A

Q16 - 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.

N/A

Q17 - 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/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			

Q17.1 - 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:

N/A

Q17.2 - To the extent you deem it necessary, please explain your reasoning for your answers to question 17:

N/A

Q18 - 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.

FESE considers that a one-size-fits-all model for duration and recovery would not be suitable. Moreover, any regulatory measures in this space would need to be sufficiently broad to allow flexibility to new types of situations and issues, recommending specific and quantitative parameters should thus be avoided.

It is very important that different approaches, in line with the different needs of exchanges are allowed. Exchanges avail of a number of mechanisms to safeguard trading and price discovery and their discretion should not be limited by overly prescriptive regulatory measures when it comes to the functional design, application and interplay of cyber-resilience measures. FESE considers that the RPO should be the point in time when the market operator is comfortable that it can ensure again a fair and orderly market.

On a general basis, financial market infrastructure operates under a 2-hours RTO guidance, as per CPMI-IOSCO Principles of Financial Market Infrastructure. 2-hours RTO guidance works well under operational disaster recovery plans, but we consider that mandating RTO under specific legislation would be counterproductive. In the wake of a cyber-incident, firms may find themselves torn between a commitment to availability for customers, completing a thorough investigation of the extent of the compromise, and ensuring the integrity of seemingly untouched systems. In an ecosystem of interconnected entities, the risk of contagion should not be underestimated. Mandating 2-hours RTO under a specific legislation would place undue pressure on firms to bring systems up, therefore risking the contagion to other firms and potentially causing a systemic event.

Q19 - 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?			

Q19.1 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:

N/A

Q19.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 19:

N/A

Q20 - Is your organisation currently subject to ICT and security incident reporting requirements?

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

Q20.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 20:

N/A

Q21 - 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

Q21.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 21:

Financial market infrastructures are subject to strict and detailed incident reporting requirements, which are mandated by their primary regulator in the jurisdiction they operate. This regime has been in place for many years and has worked well so far. Changing the approach to create a centralized reporting structure, while seemingly an attractive option because of the uniformity, might in reality introduce problems due to lack of detail and familiarity with local markets. Primary financial regulators in the jurisdiction they operate should be the parties responsible for all incident reporting requirements, as that removes the extra burden of financial entities' having to deal with multiple regulators for the purpose of reporting the same incident.

In considering ICT and security incident reporting for financial entities, both the principles of proportionality and subsidiarity, as foreseen by the Treaty of the European Union, should be considered, as well as the need to ensure a level playing field.

Firstly, it would not be proportional to make all financial entities subject to the same levels of reporting requirements without distinguishing between their levels of size, type, specificities and criticality to EU markets.

Secondly, where national competent authorities (NCAs) can supervise, this should be encouraged rather than centralising all levels of supervision. This is important as NCAs have the knowledge of local markets and their specificities. Rather than calling for harmonisation, supervisory convergence should be encouraged.

Thirdly, there is a need to ensure that levels of supervision follow the principle of "same business same rules", ensuring that regulation is technology neutral.

Instead of establishing a harmonised EU wide system, focus should be on strengthening supervisory convergence to ensure there is a level playing field across the EU.

Additionally, it could be helpful to conceive a consistent terminology as well as consistent formats for reporting events. For instance, in the NIS Directive context, each country is requesting incident reporting in different formats using different tools. This makes it difficult and time consuming to report a cross-border incident.

Q22 - 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			

Q22.1 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:

N/A

Q22.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 22:

N/A

Q23 - 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.

N/A

Q24 - 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

Q24.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 24:

In line with our reply to question 21, we believe that there should be no reporting at EU level, given existing detailed reporting at national level.

Only high severity incidents should be reported to national competent authorities. Financial entities operate their incident response framework, and the severity of the incidents is determined by specific criteria. For cyber incidents, there are two factors which should be considered as relevant in determining the materiality thresholds:

- Was the incident impactful?
- Was the incident caused by a threat actor which had a targeted and malicious intent?

Using the criteria above, only incidents that are both impactful and have targeted and malicious intent should be considered as reportable.

Q25 - 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.

FESE would not support direct supervision at central level of all financial entities. In terms of governance, division of responsibilities between competent authorities should follow a proportional approach. Moreover, it should be considered that creating a central hub of security incidents may, depending on the information contained therein, in itself become a target for cyberattacks. However, information sharing and supervisory convergence measures for competent authorities should be encouraged.

Q26 - Should a standing mechanism to exchange incident reports among national competent authorities be set up?

☐Yes
☒No
☐Don't know / no opinion/not relevant

Q26.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 26:

No, we consider a standing mechanism to exchange incident reports among national competent authorities to be unnecessary. While it would be desirable for NCAs to exchange themes of the types of incidents they are observing in their respective jurisdictions, it would be counterproductive and run against confidentiality requirements to share by default the details of the incidents reported by financial entities in their respective jurisdictions.

Q27 - 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.

Q28 - Is your organisation currently subject to any ICT and security testing requirements?

☒Yes
☐No
☐Don't know / no opinion/not relevant

If the answer is yes:

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

Q28.3 - To the extent you deem it necessary, please explain your reasoning for your answers to question 28 (and possible sub-questions):

FMIs, especially those that operate in multiple jurisdictions, are subject to multiple security testing requirements, such as CFTC Systems Safeguard Testing Regulation, Bank of England CBEST testing, Dutch National Bank TIBER NL, etc. Regulatory requirements for security testing shouldn't be prescriptive; rather, they should be principles- and outcome-based. This would allow firms which report to multiple regulators to meet their security testing requirements without having to perform a dedicated test, as mandated by each regulator. Furthermore, regulators across multiple jurisdictions should work to harmonise their testing requirements, and then develop principles and requirements that firms should meet when conducting such tests. It should be left to the firms to conduct such tests, whereas regulators should ensure that their principles are met and that findings are remediated in a timely manner, without being involved in every phase of conducting the tests.

Overall, FESE considers that cooperation between regulators and supervisory convergence are beneficial but does not see a need for a common EU framework. We consider that requirements should be streamlined where possible but also well adapted to local markets and practices.

Q29 - 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*
Gap analyses?		X	
Compliance reviews?		X	
Vulnerability scans?	X		
Physical security reviews?	X		
Source code reviews?	X		

Q29.1 - 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:

The baseline testing/assessment referred to in question Q29 is already performed at national level and should not be duplicated at EU level. What could be usefully done by the EU is to promote convergence of terminology and practices among Member States.

Regarding the questions on gap analyses and compliance reviews, while it is not clear what these covers, the principle of proportionality has to apply in all cases.

Q29.2 - To the extent you deem it necessary, please explain your reasoning.

N/A

Q30 - 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)?	X		
Impact – related factor (criticality of services provided)?	X		
Financial stability concerns (Systemic importance for the EU)?	X		

Q30.1 - Are there any other appropriate qualitative or quantitative criteria and thresholds? Please specify which one(s) and explain your reasoning:

N/A

Q30.2 - To the extent you deem it necessary, please explain your reasoning.

In considering which financial entities that could become subject to more advanced testing, both the principles of proportionality and subsidiarity should be considered, as well as the need to ensure a level playing field.

Firstly, it would not be proportional to make all financial entities subject to the same levels of requirements without distinguishing between their levels of size, type and criticality to EU markets.

Secondly, where national competent authorities can supervise, this should be encouraged rather than centralising all levels of supervision. This is important as NCAs have the knowledge of local markets and their specificities. Rather than calling for harmonisation, supervisory convergence should be encouraged.

Thirdly, there is a need to ensure that levels of supervisions follow the principle of “same business same rules”, ensuring that regulation is technology neutral.

Q31 - 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?			

Q31.1 - To the extent you deem it necessary, please explain your reasoning.

Regulators across multiple jurisdictions should harmonise their requirements for advanced testing (such as threat-led penetration testing), but responsibility should be for the primary regulators in their respective jurisdictions (national competent authorities) to oversee testing principles and requirements. Because of the scale and to deal with the issue of “concentration of expertise,” advanced testing should be the responsibility of individual firms, while regulators would draft principles and requirements for testing and/or track remediation of findings, but not be involved directly with running and closely overseeing every phase of the tests. One major benefit of leaving it to individual firms to conduct their own tests is that the frequency of those tests is likely to increase, which has the benefit of frequent and increased probing of defences. Threat-led penetration testing, which more closely can be defined as Red Team adversarial simulation, should be run on live systems, while application-specific penetration tests should be run on non-production systems.

Q32 - 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

Q32.1 - What other frequency of running such more advanced testing given their time and resource implications would be the most efficient?

N/A

Q32.1 - To the extent you deem it necessary, please explain your reasoning for your answer to question 32:

N/A

Q33 - 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)?			

Q33.1 - Is there any other element that could have a prudential impact?

Please specify which one(s) and explain your reasoning:

N/A

Q33.2 - To the extent you deem it necessary, please explain your reasoning for your answers to question 33:

N/A

Q34 - 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.

N/A

Q35 - 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

Q35.1 - 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).

N/A

Q36 - 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.

N/A

Q37 - 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?		X	
Should it focus on critical ICT third party providers?		X	
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 organizational 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)?			

Q37.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 37:

This is already done on a national level and dealt with by companies themselves when they operate cross-border.

Q38 - 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?			

Q38.1 - 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:

N/A

Q38.2 - To the extent you deem it necessary, please explain your reasoning for your answer to question 38:

N/A

Q39 - 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

Q39.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 39:

The finance sector has in recent years developed advanced sharing and voluntary exchange of information via industry led organisations, at a global, regional and national level. Examples include: FSISAC EU, WFE Global Exchange (GLEX) Cyber Security Working Group, FSCCC (in UK), etc. These existing industry forums are sufficient.

Q40 - 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:

N/A

Q40.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 40 (and its possible sub-question):

N/A

Q41 - 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:

N/A

Q41.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 41(and its possible sub-question):

N/A

Q42 - Do you consider you need more information sharing across different jurisdictions within the EU?

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

Q42.1 - 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:

N/A

Q43 - 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:

N/A

Q43.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 43 (and its possible sub-question):

N/A

Q44 - 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?

N/A

Q45 - Where do you see challenges in the development of an EU cyber insurance/risk transfer market, if any?

	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			

Q45.1 - 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:

N/A

Q45.2 - 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.

N/A

Q46 - 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 should provide any kind of support to develop EU or national initiatives to promote developments in this area, please explain your reasoning and provide examples:

N/A

Q46.1 - To the extent you deem it necessary, please explain your reasoning for your answer to question 46 (and possible sub-questions):

N/A

Q47 - Does your organisation fall under the scope of application of the NIS Directive as transposed in your Member State?

☐Yes

☐No

☒Don’t know / no opinion/not relevant

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

N/A

Q47.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 47 (and its possible sub-question):

Given that all EU Member States have transposed the NIS Directive, and Switzerland has developed a National strategy on the security of network and information system, many FESE Members report that they have been identified as operator of essential services. Those who have been identified as such, reported increased security requirements as well as enhanced reporting obligations (e.g. incident notification). Overall, FESE Members have not reported a significant impact of the NIS Directive over their cybersecurity strategy due to already existing solid and effective principles and procedures before the introduction of the Directive, based on international security standards and regulatory requirements in place, including those stemming from MiFID II/MiFIR .

Q48 - How would you assess 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 specialist clause?

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

FESE Members who have been identified as operators of essential services under the NIS Directive reported increased security requirements and enhanced reporting obligations. Overall, FESE Members have not reported a significant impact of the NIS Directive over their cybersecurity strategy due to already existing principles and procedures before the introduction of the Directive, based on international security standards and regulatory requirements in place, including those stemming from MiFID II/MiFIR.

Q49 - 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:

N/A

Special question: in order to select the next questions what 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 50-51 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**

Q50 - Did you encounter difficulties 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:

N/A

Q51 - How do you cooperate with the NIS competent authority in the Member State where you are established? Do you have agreements for cooperation/MoUs?

To the extent you deem it necessary, please explain your reasoning and provide details on your experience:

N/A

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

Q52 - 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.

N/A

Q53 - 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.

N/A

Q54 - 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 to question 54, please explain those particular issues:

N/A

Q54.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 54:

N/A

Q55 - Have you encountered any issues in matters involving cross-border coordination?

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

If you answered yes to question 55, please explain which issues.

N/A

Q55.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 55:

N/A

Q56 - 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.

N/A

Q57 - 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.

N/A

Q58 - 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.

N/A

Q59 - 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:

N/A

Q60 - 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:

N/A

Q61 - 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:

N/A

Q62 - 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

If you answered yes to question 62, to the extent possible, please provide any useful information (in relative or absolute) terms that you may disclose:

N/A

Q62.1 - To the extent you deem it necessary, please explain your reasoning for your answers to question 62 (and its possible sub-question):

N/A