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

---

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	**X**
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:
Given the current threat landscape, financial entities should have an ICT and security risk management framework in place based on key common principles that are aligned with existing internal and external threats. This is important to ensure business continuity, data and process integrity, and reliability. It is vital for the security of financial institutions to have an extensive ICT and security risk management framework consisting of preventive, detective and responsive controls including 'testing'.

The Netherlands places great importance on information security frameworks and standards, which can be seen as key common principles, and actively encourages firms to apply them. Examples of important frameworks and standards are NIST, COBIT, ISO27001 and ISO27002, the CPMI-IOSCO guidance on cyber resilience for financial market infrastructures, the DNB Good Practice Information Security and the EBA guidelines on ICT and Security Risk Management. Because of this importance, the Netherlands also actively participates on the EU-level and beyond, in drafting guidelines, frameworks and standards, such as the EIOPA Guidelines on ICT & Security.

Question 2 – 17
[niet van toepassing]

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.
The following can be taken into consideration. A requirement that financial institutions develop RTO's and RPO's as a general principle is a good idea. However, we do not see merit in quantifying such objectives, because of the differences between organizations caused by many factors, such as size and type of services provided. There should be an element of proportionality. The duration of the RTO should depend on the importance and criticality of the process or system ('societal business impact assessment'), which may vary between institutions depending on the specific risk profile. For example: the business risk profile of an insurer or a pension fund is different from a bank or service payment provider. Business continuity of insurers and pension funds is important, but less time sensitive than business continuity of payment systems.

Question 19-20
[niet van toepassing]

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	**X**
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:
The implementation of such a system if properly and efficiently implemented would have

merit, however, the phrasing of the question is quite absolute, and we believe the extent to which such a system should be implemented requires further research. That said, a comprehensive and harmonized EU-wide system of ICT and security incident reporting would be consistent with one of the recommendations made by the European Supervisory Authorities (ESA's) in their advice to the European Commission (EC) of April 2019. Currently, financial entities have to report ICT and security incidents to multiple supervisory authorities in different formats, with sometimes inconsistent terminology, and different timeframes. This harbors the risk of inefficiency and ineffectiveness, which could be mitigated by the harmonisation, streamlining, and standardisation of templates, taxonomy, and timeframes for incident reporting. Such a system has to take into account the differences between entities, (services risk based approach) and proportionality in general, so as to relieve the administrative burdens caused by the current diversity. Furthermore, incident reporting could help competent authorities and financial institutions to log, monitor, analyze and respond to ICT risks.

Additionally, it might be of interest to note that the Dutch central bank (DNB) chairs the EIOPA Working Group on IT & Security, which has 'incident reporting' as one of the workstreams. The working group is currently drafting an advice for a simplified, essential, harmonised, and shared framework for incident reporting within EIOPA, to be used for cyber underwriting.

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	**X**		
Reporting templates	**X**		
Reporting timeframe	**X**		
Materiality thresholds	**X**		

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:
As stated in the explanation to question 21, the extent to which such a system should be implemented would warrant further research. However, were such a system to be implemented it would be logical to harmonise the abovementioned elements. In regard to reporting templates, the template could include a sufficient amount of details, e.g., root cause, incident impact, influenced services, related problems/errors, "3rd parties involved"/relations with/interconnected to other financial institutions. This could be important information for analysis and assessing impact. Furthermore, it could be important for a new and harmonised EU-wide system to include provisions to ensure that relevant national supervisory authorities are informed of any ICT and security incidents, in order to allow the supervisory authorities to exercise proper supervision.

Question 22.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 22:
The materiality thresholds should be qualitative because of the diversity between the institutions, which makes a uniform set of quantitative thresholds difficult to implement and undesirable.

As to the information in the report, it is important to include relevant information on threat actors, any signals regarding the quality of the implemented IT-general controls (IAM, change management problems, software developments issues, etc.) and application control problems in order for the supervisory authorities to assess the impact of incidents for the reporting entity and the sector as a whole.

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.
A good example of a template that provides the appropriate level of detail are the template included in annex I of the EBA Guidelines on major incident reporting, and the ITIL framework. Generally, details should include (inter alia):

- contact person institution;
- type of institution;

- reference number;
- method of notification;
- date/time recorded;
- description incident categorization;
- incident impact;
- influenced services;
- activities undertaken to resolve the incident;
- resolution date and time;
- incident status;
- related problem/known error;
- verified/probable root cause;
- name of the person recording the incident.

There are two main perspectives relevant for reporting IT related incidents, which are the governance point of view and the IT point of view. Different stages of the incident process (identification, respond, resolve) require different information. An incident report is not only relevant to assess the IT-related risk management/security framework and the potential risk of the threat to other firms, but also to assess the adequacy of the enterprise/operational risk framework in general.

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	**X**
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:
Incident reporting is an important tool for supervisory authorities to gain more insight into the risk management cycle of firms. Obligatory reporting of minor incidents, however, would result in disproportional administrative burdens for the sector as well as the supervisors. Thus, there should be materiality thresholds on a qualitative, as opposed to quantitative, basis. Factors such as data security, reputation risk, and overall trust in the financial sector should, for example, be taken into account.

Secondly, including all incidents within the scope of reporting might have the adverse effect that entities will avoid logging minor incidents, as the administrative burden outweighs the actual benefit of logging. Moreover, for proper incident reporting an adequate, uniform definition of 'incident' is needed.

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.
Adequate confidentiality and access controls are important governance elements for ICT and security incident reporting. In addition, reporting requirements could be standardised through more EU coordination. A single authority to act as a control FI hub or database could have its benefits, such as enhanced cross-border cooperation and information sharing, but requires further investigation.

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

Yes	**X**
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:
This relates to the answer given in question 25. In any case, the sharing of information regarding security incidents helps to mitigate and counter security threats. NCA's should under all circumstances have access to the shared incident reports.

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.

A factor that might hinder information sharing is a lack of assurance for the financial institutions themselves, with respect to confidentiality and access restrictions of the information they share. These factors might make them reluctant to share such information as they might expose weaknesses.

Question 28
[niet van toepassing]

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?	**X**		
Compliance reviews?	**X**		
Vulnerability scans?	**X**		
Physical security reviews?	**X**		
Source code reviews?	**X**		

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:
Depending on the size of the entity and other proportionality considerations, entities should include the security of their critical/important service providers in their baseline testing and assessment framework. In addition, (advanced) red teaming requirements could be included for (systemically) important entities.

Question 29.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 29:
All the above elements add to the strengthening of operational resilience. Source code reviews could contribute to the maintainability of source code and avoiding/repairing so called 'spaghetti code', meaning unstructured and difficult-to-maintain source code, which can be caused by, for example, volatile project requirements, lack of programming style rules, and insufficient ability or experience. Regarding source code reviews, however, it is important to consider proportionality in a specific case.

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

Question 30.1 Are there any other appropriate qualitative or quantitative criteria and thresholds? Please specify which one(s) and explain your reasoning:
Another relevant requirement is the presence of confidential data.

Question 30.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 30:
All three of the criteria are relevant testing requirements. In regard to advanced testing, a suitable model for increasing digital resilience across the EU is TIBER-EU (which supports pan European testing and mutual recognition).

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?		**X**	
Should it be focused on live production systems?	**X**		
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?	**X**		
Should testers be certified, based on recognised international standards?	**X**		
Should tests run outside the Union be recognised as equivalent if using the same parameters (and thus be held valid for EU regulatory purposes)?		**X**	
Should there be one testing framework applicable across the Union? Would TIBER-EU be a good model?	**X**		
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?		**X**	
Should more advanced testing (e.g. threat led penetration testing) be compulsory?		**X**	

Question 31.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 31:
The Netherlands finds it important to have a single testing framework applicable across the EU to enable cross-border testing, and believes TIBER-EU to be a good model, which has been rolled out in ten EU jurisdictions already. Testing should, however, not be run on all functions, but should focus on critical functions. In this regard the definition used in the TIBER-EU framework is relevant: "the people, processes and technologies required by the entity to deliver a core service which, if disrupted, could have a detrimental impact on financial stability, the entity's safety and soundness, the entity's customer base or the entity's market conduct." A test could, besides the critical functions, also have business critical functions in scope. This would focus on functions that would not directly impact the sector as a whole but, if hit, would be disastrous for the institution itself and therefore could lead to a loss of trust and reputation in/of the sector as a whole. Furthermore, to gain the most benefit out of TIBER-EU test, it must be focused on live production systems, as hackers are focused on that too.

With regard to testers, it is important to have independent external testers to execute the TIBER-EU test, to increase objectivity, and to prevent any known or unknown biases, or knowledge of the system, to interfere with the quality of the testing. This is also mandatory under the TIBER-EU framework.

With regards to certification, it could be important to establish a certain quality level, however, it might in practice be quite difficult to set up and maintain proper certification, and would limit the options for parties to perform such tests. Furthermore, tests run outside the EU should not in principal be recognised as equivalent as tests are not standardized enough to agree to mutual recognition upfront. Even frameworks with the same principles differ wildly in execution. Although, it would be possible with TIBER-EU because of the strict mandatory elements and constant contact between the different TIBER cyber teams using TIBER-EU's knowledge centre as a pivoting point.

While involvement of the ESA's and other EU-bodies could be useful for cross-border coordination there is no need at this moment to develop another framework beside TIBER-EU. TIBER-EU should be not compulsory for systemically important institutions, as the learning experience is much higher when the testing is done on a voluntary basis. Of course, moral suasion may be used to involve as many institutions as possible. E.g. every authority should check which institutions are most critical in its sector and bring them together to discuss and consult the sector on where they see the most added value can be gained from performing these kinds of tests. All ten jurisdictions that up until this point in time have set up a TIBER-EU

based framework have done so on a voluntary basis. If TIBER-EU would be compulsory, the learning experience of these institutions will not be stimulated as much as possible, especially when it comes to learning by sharing experiences within the sector. An important benefit of voluntary TIBER-EU testing is the information sharing between institutions, creating a trusted community. Trust cannot be mandated by a supervisor.

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	**X**
Other	

Question 32.1 To the extent you deem it necessary, please explain your reasoning for your answer to question 32:
Given its time and resource implications, a TIBER-EU test should occur once every three years. It takes a significant amount of effort and time to implement 'lessons learned' and findings of a TIBER-EU test. However, in the multiyear period between TIBER-EU tests, less time and resource consuming testing could be in place for 'significant' financial entities. For these entities 'pentesting' and regular red teaming, for example, should be standard business practice.

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 [illegible])	**X**		
More advanced testing (e.g. TLPT)?	**X**		

Question 33.1 Is there any other element that could have a prudential impact? Please specify which one(s) and explain your reasoning:
Sharing within the sector of played scenarios, best practices, and remediation actions, can benefit not only the tested entity but the sector as a whole.

Question 33.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 33:
Both elements can have a prudential impact.

Question 34-35
[niet van toepassing]

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.

It could contain provisions pertaining to the following, but further research is required:

- information and audit rights as well as control possibilities for the supervised entity, unrestricted by contract;
- Information and audit rights as well as control possibilities for the supervisory authorities;
- duty to inform supervised entity of information it needs to adequately control and monitor the risks associated with the outsourcing;
- Requirements regarding proof/certificates and audit reports;
- Rights of the supervised entity to issue instructions;
- Obligations in regard to data security/protection (reference to location of data storage);
- Termination rights and adequate termination notice periods;
- Provisions on the possibility and the modalities of chain-outsourcing ensuring that relevant legal requirements are not impeded, including an obligation to inform/seek prior approval of the supervised entity;
- Provisions are to be agreed ensuring that the cloud service provider informs the supervised company about developments that might adversely affect the orderly performance of the outsourced items;
- Choice of law clause, i.e., the law of a country from the EU or EEA;

- Choice of forum clause, i.e. the courts of a country from the EU or EEA.

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?			**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.)?	**X**		
Should proportionality play a role in the identification of critical ICT third party providers?	**X**		
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?	**X**		
Should EU and national competent authorities responsible for the prudential or organisational supervision of financial entities carry out the oversight?			**X**
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)?			**X**
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.)?			**X**
Should it also include binding tools (such as sanctions or other enforcement actions)?			**X**

Question 37.1 To the extent you deem it necessary, please explain your reasoning for your answers to question 37:
The question as to whether or not an oversight framework should be introduced, as well as how that oversight framework should work in practice, warrants further research. That said, we recognize the importance of this subject, as some ICT third party providers, especially the very large service providers, could have a lot of influence on financial entities through (for example) cloud computing solutions, data services, as well as through licensing models, and, more generally, market power. Currently, most ICT third party providers could have some, direct or indirect, influence on the stability of the financial sector in Europe. Due to their possible market power and the cross-border nature of ICT third party providers, more coordination, cooperation and supervision on an EU level might be needed (similar to the oversight of SWIFT). This is in line with the advice of the ESA's to establish an oversight, or other, framework for critical third party providers. In this regard it could be important to not only focus on ICT-providers, but all critical third party providers.

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)		**X**	
Mandatory multi-provider approach		**X**	
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?			**X**

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:
The lack of technical standardisation among ICT third party providers results in a lack of

portability and interoperability, which results in 'vendor lock-in' risks for financial entities. For example, varying terms of service in regard to which default configuration settings are used. Encouraging technical standardisation among ICT third party providers may alleviate some of these concentration risks.

Question 38.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 38:
Diversification strategies, including a potential mandatory or voluntary rotation mechanism with associated rules to ensure portability, or a mandatory multi-provider approach, is likely to lead to higher ICT expenditures of financial entities, and would not necessarily lead to less concentration risk due to third and fourth party dependencies on the same ICT third party service providers. For example, if most sub-contractors of a financial entity are dependent on the same hyperscale cloud service providers, a rotation mechanism or a mandatory multi-provider approach would not resolve these inherent concentration risks when a few major tech companies together represent a supermajority of all cloud services worldwide, and these service providers are not easily substitutable.

In general: It is very important for the outsourced institution to have a credible exit plan, either by swapping third party or taking the service in-house. The mentioned requirements in question 38 are quite heavy. A balance between mitigating the risks and the workings of a free market would be optimal. Apart from the risks, outsourcing ultimately has many advantages as well.

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	**X**
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:
The cross-border nature of ICT solutions as well as of the financial institutions themselves make it important for the EU to have a role in supporting such exchanges, especially considering that the institutions might be hesitant to undertake voluntary exchanges on their own.

Questions 40-44
[niet van toepassing]

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

	Yes	No	Don't know/no opinion/not relevant
Lack of a common taxonomy on cyber incidents		**X**	
Lack of available data on cyber incidents		**X**	
Lack of awareness on the importance of cyber/ICT security		**X**	
Difficulties in estimating pricing or risk exposures	**X**		
Legal uncertainties around the contractual terms and coverage	**X**		

Question 45.1 Is there any other area for which you would see challenges in the development of an EU cyberinsurance/risk transfer market? Please specify which one(s) and explain your reasoning:
It could prove difficult to specify adequate terms and conditions for cyber insurance and related risk transfer implications in the EU, and furthermore there could be an element of self-fulfilling prophecy, where the amount of ransom claimed could be the insured amount.

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:
Coverage can be problematic since cyber risks keep evolving. New techniques are being developed constantly. Another difficulty is in determining (degrees of) culpability for the damage, such as, for example, when an entity has questionable cyber resilience practices in place.

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

Yes	**X**
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:
Although we currently do not see any major issues, if there is a specific need for the development of an EU cyber insurance/risk transfer market, it would stand to reason if the EU is involved given the cross border nature of such a market, as well as of the risks and the relevant entities.

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

Question 47-51
[niet van toepassing]

Question 52. Do you receive NIS relevant information in relation to a financial entity under your remit? Please detail your experience, specifying how this information is shared (e.g. ad hoc, upon request, regularly) and providing any information that may be disclosed and you consider to be relevant:
The Dutch supervisory authorities (the Dutch Central Bank (DNB)) and the Netherlands Authority for the Financial Markets (AFM)), receive information regarding incidents from financial institutions under their supervision. DNB is both financial supervisor and designated NIS competent authority, and is able to share information.

Question 53. Would you see merit in establishing at EU level a rule confirmingthat 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:
Yes, supervision of relevant ICT and security risk requirements is an integral part of financial supervision. Therefore, they should be an integral part of the supervision by the same authority that is supervising the other risks.

Questions 54-55
[niet van toepassing]

Question 56. What is your experience with the concrete application of the lex specialis clause in NIS? Please explain by providing, whenever possible, concrete cases where you either found the application of the lex specialis helpful, or otherwise where you encountered difficulties or faced doubts with the application or interpretation of specific requirements and the triggering of the lex specialis:
The Netherlands made use of this clause, with reference to existing acts and regulations, by exempting financial institutions from the security requirements imposed in the NIS directive. This has proven to be useful. It also means that the supervision of ICT and security risk of banks under the NIS can rely on the supervision of ICT and security risks under CRR/CRD.

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:
Both in the short term and in the medium to long run, investments seem to be necessary to keep EU financial institutions at adequate levels of cyber resilience.

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:
Although this requires further research, streamlining reporting requirements and more international coordination and cooperation to address the risks posed by third party providers could be beneficial.

Streamlining reporting requirements could lead to a one-off investment, with increased efficiency in the long run because of a decreased administrative burden for institutions. International coordination and cooperation could lead to increased efficiency and effectiveness in supervision.

Questions 59-62
[niet van toepassing]