Brussels, 19 March 2020
FINAL

EACB response to the EC's Online Public Consultation on a digital operational resilience framework for financial services: making the EU financial sector more resilient and secure

The **European Association of Co-operative Banks** (EACB) represents, promotes and defends the common interests of its 27 member institutions and of cooperative banks, with regard to banking as well as to co-operative legislation. Founded in 1970, today the EACB is a leading professional lobbying association in the European banking industry. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 2.800 locally operating banks and 51,500 outlets, they serve 209 million customers, mainly consumers, SMEs and communities. Europe's co-operative banks represent 84 million members and 713,000 employees and have an average market share in Europe of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Questions

2.1. ICT and security requirements

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?

X	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.*

We welcome the initiatives towards EU-wide uniform security standards and the harmonisation of supervisory practices. It is important to regulate and monitor the security of financial systems in a holistic framework.

Given the reliance of the financial sector on IT, the risks involved should be covered accordingly. Proper IT (security) risk management practices are crucial.
It is necessary that everyone involved takes responsibility for IT security and potential cyber risks.

Uniform guidelines should fit into a uniform supervisory concept towards financial service providers and banks. Specialised business guidelines on information security (payment transactions, securities, risk management) should also be included in this set of rules.

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.*

Considering the principle of proportionality, RTO and RPO are bank-specific and risk-oriented. We believe that a standard RTO would not fit every business process involved because it is inherently related to each bank's risk-appetite and exposure.

Moreover, if the Commission is considering regulating this on level 1, we would like to remind the Commission that banks already have operational requirements coming from guidelines and practices.

In a nutshell, we believe that regarding RTO and RPO, legal or regulatory requirements are not needed.

2.2 ICT and security incident reporting requirements

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?

X	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.*

The reporting of IT security incidents should be carried out by a uniform scheme via a single reporting channel and be forwarded to all authorised bodies. A harmonisation of the reporting requirements is welcome – taking into account all participants in the financial system.

This could help financial institutions share data and detect problems others have had/are experiencing.

The reporting would also be beneficial for external communication.

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

As said in our answer to Question 21.1, we think that a single reporting channel (point of contact) to the relevant authorities would be beneficial.

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.

N/a.

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.*

Concerning the level of detail, we believe that the report should contain information on time, type of attack and used resources to establish the breach. This could help other entities to prevent a a successful reoccurrence of the attack.

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
X	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.*

Incident reporting should be limited to significant security incidents that may affect the security of supply to the public or the stability of the financial system or that may affect other banks. Reporting of mere operational incidents that do not meet these criteria should be avoided.

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.*

All organisations require a certain level of transparency when it comes to security incidents. Past experience shows that the more governance bodies are involved, the less transparency is achieved. As said in our responses to Questions 21.1 and 22.1, a single reporting channel (point of contact) to forward/share/distribute reports to the relevant national supervisory authority and vice versa would be beneficial.

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

X	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.

Further explanations are not necessary.

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.*

1. A non-standardised taxonomy.
2. Non-standardised templates.
3. Lack of a central coordination point.

2.3. Digital operational resilience testing framework

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

N/a.

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.*

All financial institutions should take appropriate action (analysis, assessments, and information security/cyber tests) to ensure the effective identification of vulnerabilities in their ICT systems and services based upon their risk appetite and specific business. This would mean that a baseline could differ and focus on risks determined by the company.

We have no detailed specification of the concrete methods to indicate, since the choice depends on the criticality and the circumstances (e.g. source code review for related software is not possible).

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

No.

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.*

TLPTs are good building blocks for an effective legal protection insurance and should be supported depending on the criticality/significance, especially for systems that are necessary for the security of supply to the population and financial stability.

The participation of institutes in special red teaming tests (e.g. according to the TIBER EU framework), with the participation of supervisory authorities, should be voluntary.

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

Concerning the entry "Should testers be certified, based on recognised international standards?", we would like to specify that there is no need to regulate at this level as this best practice should be left to individual banks.

Concerning the entry "Should there be one testing framework applicable across the Union? Would TIBER-EU be a good model?", we want to stress that TIBER-EU is a valuable but, importantly, voluntary framework currently available on the market.

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

If "Other", question 32.1 What other frequency of running such more advanced testing given their time and resource implications would be the most efficient? *5000 character(s) maximum including spaces and line breaks, i.e. stricter than the MS Word characters counting method.*

The relevant institutes should independently implement and control the tests in the overall test concept (no fixed schedule). However, a cycle of approximately three years might be more efficient in order to give the organisation enough time to implement.

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

N/a.

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.*

It has to be ensured that the various procedures for checking the effectiveness of security measures are used in a balanced ratio. Cyber-attack strategies are continuously changing and new security gaps occur in financial markets. That is why continuous monitoring and regular (cost-effective) measures are necessary.
Advanced test methods like TLPTs provide financial entities with well-established information security management, additional insights into the state of cyber resilience and direction on improvements to be made.

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 setup and management of contractual arrangements with third party providers, also enabling a better overview of risk 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 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?

X	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.*

Each country has its own regulatory requirements. An example is the location of data storage. Some of the local regulators demands that data is stored within the same country. This can be very challenging for cloud providers if they do not have a data centre in that specific country.

Moreover, our members have experienced difficulties during contractual negotiations between their organisation and third party ICT providers especially concerning the agreement on inspection rights with potentially high conflict. Banks' on-site audit right has been one of the most challenging topics in contract negotiations, followed by audit rights, data location (as mentioned previously), sub-outsourcing, agreement or transparency on security targets and the monitoring of their implementation, particularly in the area of Public Cloud Service Providers. Finally, our members have had issues with small and mid-sized outsourcing providers as it is difficult to get the agreement for their supervisors' requirements.

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.*

Outsourcing is a sensitive issue for co-operative groups and networks, whose organisational structure relies on a division of tasks. Due to their distinctive "division-of-labour" structures, group/network entities or central institutions provide numerous services for affiliated banks. This traditional supporting pillar finds its basis in national legal frameworks. For example, the laws and statutes governing local co-operatives or their central institutions or associations regularly stipulate that the central support services organised in the respective network are to be offered by the central institution or used by the local banks belonging to the network. Such organisational structures, especially the bundling of tasks in specific entities, improve their cost efficiency and achieve economies of scale.

In our view, Cloud Service Providers (CSPs) should have the same execution framework with all their clients (including banking institutions) and should be certified by a regulator. As the EC has already begun to work on the matter, their initiatives could be extended to define: Standardised

terms and conditions integrating all the provisions proposed by the EBA regarding access and audit rights, security of data and systems, location of data and data processing (including sub-processing), chain outsourcing, contingency plans and exit strategies (e.g. rights to termination; resolution clauses; business continuity and contingency clauses); standardised level of security depending on the business concerned. Moreover, in November 2019, the EU Single Resolution Board (SRB) had a consultation on their paper: 'Expectations for banks' which put forward requirements for banks and their access to FMIs in case of a default etc. The SRB highlighted that banks shall ensure the continued provision of critical services that support critical functions, also in resolution. Usually the critical services have some link to clouds and therefore this rule is critical and should be included in relevant outsourcing agreements.

The compliance with this framework should not be placed on banks exclusively as they do not have the ability to impose their conditions to CSPs.

Finally, we think that financial entities as well as third party ICT providers and the EC should refer to the ISO / IEC 27017: 2015 when discussing contract clauses. This standard would be appropriate, because comparing it to the ISO / IEC 27002 and ISO / IEC 27001 standards, it contains guidelines on aspects of information-security in cloud computing.

For each area of the higher-level standard ISO / IEC 27001, possible peculiarities of cloud security are explicitly explained. This methodology enables security targets to be identified more quickly and integrated into the security management system.

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

We believe that an oversight framework for critical service providers would be beneficial for the financial sector. This should not imply that a new oversight framework should increase the banking and financial sectors obligations and supervisions as the sector is already heavily regulated also with the recent requirements of the 2019 EBA Guidelines on outsourcing arrangements.

Considering the various options, should the selected standard framework be an EBA regulation, this will strengthen financial sector capacity to negotiate, but will not always be imposed on CSPs since they are not in the supervision field of the EBA. The need would be to obtain a regulatory framework that could legally embed providers in the application of the major mandatory cloud clauses.

A complementary approach to be considered could be the one to obtain a Trustworthy European Cloud for the financial sector with the creation of a label relating to cloud categories (to define) and according their criticality. This label should include a list of criteria which would come from legal technical security requirements (e.g. the 2019 EBA Guidelines). The providers would be forced accordingly to adopt the Cloud "by design" for the banking and financial sector.

Concerning the various entries of the table, on the "criticality" aspect, the definition of "criticality" should not disrupt the level playing field or lead to forum shopping.

We would like to generally comment that if direct supervision of third-party service providers is intended, the same rules should apply to all market participants, e.g. no sandboxes for individual FinTechs.

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

N/a.

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

Neither a rotation of providers nor a "mandatory multi-provider model" is actually feasible. We believe that banks should be free to decide concerning the most appropriate and effective solution to address concentration risks among ICT third-party service providers, depending on their business model and risk management.

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?

X	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.

In recent years, cyber attacks have occurred to varying degrees locally.

For this reason, organised exchange across national borders can be helpful in defending against such attacks, if you are not the first to be affected by a new threat.

The voluntary exchange of such information should be further promoted in order to improve the overall level of security. Cybersecurity would be improved if TTPs were shared so companies can defend themselves and improve their countermeasures.

Findings from reports by financial institutions on specific or clustered attack patterns should therefore be used for a situation report and in anonymised form as a starting point for information exchange in the financial sector.

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

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

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):

In general, sharing of incident-related technical information (for example IOCs), potentially relevant to other financial institutes, can be seen as a very positive thing.

A challenge we see is that this should be kept on a technical level, including information that could be relevant for defence or threat hunting. Sharing full incident details (for example full internal investigation reports) does not provide additional value and can lead to leaks of classified information.

In general, if we are talking about sharing IOCs for example, there are quite widely known problems with incompatibility issues between different security solutions, so finding a solution that could technically act as information sharing platform might be an issue. Every serious entity in this matter wants to automate especially the IOC fetching, so traditional "sending an excel sheet or report document with IOCs" is an old approach. The integration must happen between systems and must be automated.

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.

In general we believe that information sharing in this context is beneficial, as also explained in our previous answers. However, in order to reply to Question 42, we need further explanation and more elements to better understand the question as it is too open and vague. It implies different sub-questions and a context to fit the question in, e.g. who would be sharing the information (a national competent authority, an EU authority, a financial institution, etc), and from whom? What kind of information has the Commission in mind?; etc.

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 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 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.

We don't know.

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.

N/a.

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

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.

Cyber-insurance is one way of transferring risk. The decision to insure is institution-specific and is based on risk assessments, taking into account the proportionality principle and risk affinity.

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.

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.

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.

- Additional audit obligations with reporting to national safety authority.
- Double reporting of operational and safety incidents to the national safety authority.
- Banking supervision with different reporting schemes.

Question 49. Are you covered by more specific requirements as compared to the NIS Directive requirements and if so, do they originate from EU level financial services legislation or do they come from national law? To the extent you deem it necessary, please explain your reasoning: 5000 character(s) maximum including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

This question is more for individual banks than for an association. However, we are aware that our members are covered by more specific requirements as compared to the NIS Directive. Just to give some examples, in Germany, the implementation of the NIS Directive has been done i with the IT security law. Further specific requirements for information security management/risk management result from the banking supervisory requirements for IT (BAIT) of the Federal Financial Supervisory Authority (BaFin); in Austria the national implementation of the NIS Directive is very close to the original. However, banks are subject to further specific requirements

concerning information security (risk) management and ICT risk management stemming from competent authorities like FMA and EBA.

We also recall that banks have additional requirements stemming from the GDPR and PSD2, for example. Banks have to comply with three reporting obligations: data breach under GDPR (Art. 33), incident reporting under PSD2 (Art. 96 + EBA Guidelines on major incidents reporting under PSD2) and NIS Directive (Articles 14(3) and 16(3)). The concurrence of three notification obligations, with different deadlines, in the event of incidents with different authorities represents a considerable burden for banks.

Incident reporting under both PSD2 and the NIS Directive could also concern data breaches under the GDPR. This represents a real and factual procedural burden that is compounded by different and sometimes parallel processes for notifying breaches.

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.

- Significant increase in spending on compliance issues.
- Further restrictions on entrepreneurial decisions.
- Decline in profitability of the financial sector.
- Loss of bank diversity.

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.

No opinion.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser, Retail Banking and Consumer Policy (chiara.delloro@eacb.coop)