ÖSTERREICHISCHE FMA · FINANZMARKTAUFSICHT

OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

Europäische Kommission
Generaldirektion Finanzstabilität,
Finanzdienstleistungen und Kapitalmarktunion

SPA 2 – Pavillon Rue de Spa 2 / Spastraat 2
1010 Wien
Belgium

Via E-Mail an: fisma-crypto-assets@ec.europa.eu

BEREICH Integrierte Aufsicht
GZ FMA-LE0001.230/0004-INT/2020
(bitte immer anführen!)

SACHBEARBEITER/IN Mag. Philip Gollmann
TELEFON (+43-1) 249 59 -4213
TELEFAX (+43-1) 249 59 -4299
E-MAIL philip.gollmann@fma.gv.at
E-ZUSTELLUNG: ERsB-ORDNUNGSNR. 9110020375710

WIEN, AM 19.03.2020

EK-Konsultation: Finanzdienstleistungen – Verbesserung der Widerstandsfähigkeit gegenüber Cyberangriffen

Sehr geehrte Damen und Herren,

bezugnehmend auf die öffentliche Konsultation der Europäischen Kommission zu

„*Finanzdienstleistungen – Verbesserung der Widerstandsfähigkeit gegenüber Cyberangriffen*“

erlauben wir uns Ihnen anbei die gemeinsame Stellungnahme der **Österreichischen Nationalbank (OeNB)** und der **Österreichischen Finanzmarktaufsichtsbehörde (FMA)** zukommen zu lassen.

Selbige Stellungnahme wird zur leichteren Auswertung ebenso im Rahmen des Online-Fragebogens zur gegenständlichen Konsultation (siehe: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act/public-consultation) eingebracht.

Wir ersuchen höflich um Berücksichtigung unserer Anregungen und stehen für Rückfragen gerne zur Verfügung.

Finanzmarktaufsichtsbehörde
Bereich Integrierte Aufsicht

Für den Vorstand

MMag.a Dr.in Julia Lemonia Raptis, LLM LLM Dr. Christoph Seggermann

elektronisch gefertigt

Signaturwert	eRBEAzMTR8UT8te7JOCMaqXgRzBAgwdKBQ4U23WvI1c0KUtw7R+M5iEOTMuyWzoVRMDQl1geWL0QOB5nCvlU FnUU644YI1D04/ZUQ7qlee1bieFBeATXN1lao8tFBzgVhn2jSLv/UySxEHW5ndRA7Zi/5YmeTp98QcuDjGgV R5zhlWaGgxo3/NoOu92UCrBjW7nTY4wn4t8caL5jAzP+L1i043HpsbwNU3j7RJyY00wOVWNDR9txTfk/DMv3 qeYcrm6a43N8aE9vxbyQD1hoCGuYtr/kVlWGJgjYAgDe/Yw1/Z1QjHSbLNrrho9QpcJYoxEShW18KGU2SXI5 3d5CwQ==	
	Unterzeichner	Österreichische Finanzmarktaufsichtsbehörde
	Datum/Zeit-UTC	2020-03-19T20:20:51Z
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	532114608
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

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

CONSULTATION DOCUMENT

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

Disclaimer

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

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

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

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

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

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

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

CONTENT OF THE CONSULTATION DOCUMENT

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

Introduction

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

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

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

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

Dependence on ICT and data raises new challenges in terms of operational resilience. The increasing level of digitalisation of financial services coupled with the presence of high value assets and (often sensitive) data make the financial system vulnerable to operational incidents and cyber-attacks. While it already outspends other sectors in safeguarding itself against ICT risks (both of malicious and accidental nature) finance is nonetheless estimated to be three times more at risk of cyber-attacks than any other sector[3]. In the recent years, the frequency and impact of cyber incidents has been increasing, with research estimating the total cost in the range of tens to hundreds of billions of Euro for the global economy. The increasing digitalisation of finance is set to accelerate this trend. The ever-increasing number and sophistication of cyber-threats and ICT incidents in the financial sector illustrate the importance and urgency to tackle the incidence and effects of these risks in a pre-emptive way. Operational resilience issues, and in particular ICT and security risks can also be

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

[2] According to Statista, financial sector combined IT spending worldwide in 2014 and 2015 amounted to US$ 699 billion, well ahead of manufacturing and natural resources (US$ 477 bn), media (US$ 429 bn) or governments (US$ 425 bn). Total global IT spending in 2014 and 2015 were estimated at US$ 3734 billion and US$ 3509 billion respectively, suggesting that almost 1 in every 5 US$ spent on IT worldwide is in the financial sector.

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

source of systemic risk for the financial sector. These issues should be addressed as an integral part of the EU regulatory framework and single rulebook that aims to ensure the competitiveness, integrity, security and stability of the EU financial sector.

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

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

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

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

- strengthening the digital operational resilience of the financial sector, in particular as regards the aspects related to ICT and security risk;
- the main features of an enhanced legal framework built on several pillars;
- the impacts of the potential policy options.

Stakeholders mapping

The following relevant stakeholder groups have been identified:

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

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

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

- Industry, business associations, SMEs: financial services providers (e.g. credit institutions, (re)insurance companies, investment firms, central counterparties, central securities depositories, trade repositories, credit rating agencies, audit firms, asset managers, regulated markets, payment service providers etc.), ICT services providers.
- Consumers, financial services and ICT services users, civil society.
- Academia and public interest organisations and think tanks

Context of the present consultation

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

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

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

More specifically, they propose legislative changes in four main areas: (1) requirements on ICT and security risk management in the legislative acquis applicable to the financial sector, (2) streamlining the existing incident reporting requirements (3) setting out a cyber resilience testing framework and (4) establishing an oversight of ICT third party providers to the financial institutions.

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

In this context, the Commission is launching a public consultation to explore how an enhanced framework for digital operational resilience of the EU financial sector could be set up. This goal

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

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

[8] See https://eu2019.fi/documents/11707387/15400298/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09 S2.pdf/29565728-f476-cbdd-4c5f-7e0ec970c6c4/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09 S2.pdf

could be achieved through an EU cross-sectoral initiative for the financial sector that would take into account the strengths and specificities of existing international, EU and national frameworks and developments on ICT security and risk management.

For more information or additional questions please contact: fisma-digital-operational-resilience@ec.europa.eu

PART I

1. STAKEHOLDER IDENTIFICATION, TRANSPARENCY AND CONFIDENTIALITY

PART II

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

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

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

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

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

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

- The **development of a digital operational resilience testing framework** across all financial sectors, providing for a mechanism to anticipate threats and improve the digital operational readiness of financial actors and authorities. This assessment could look into setting key requirements to perform digital operational resilience testing while maintaining flexibility and proportionality to address specific needs of financial actors by virtue of their size, complexity and scale of operations.
- Specific rules enabling a **better oversight of certain critical ICT third-party providers** which regulated financial institutions rely on, and outsource functions to.
- Specific arrangements **to promote** a) **effective information sharing** on ICT and security threats among financial market participants and b) **better cooperation** among public authorities.

2.1. ICT and security requirements

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

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

Questions:

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

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

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

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

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Due to the reliance of the financial sector on ICT systems, a lack in cyber resilience poses a potential existential operational risk for financial market participants (FMP). Furthermore, data dependency and interconnectedness of the financial sector demand a base level of ICT security among all FMP to mitigate risks for consumers (especially data protection) and financial stability. European cyber resilience legislation should take the specific risks of the financial market into account, provide proportional rules for FMP and harmonise cyber security rules across all sectors to counteract the fragmentation of the current European legislation. All financial entities should have in place an ICT and security risk management framework. Austrian supervision backed this view by publishing respective Guides on ICT Security and for instance by taking part in EIOPA's work on drafting the proposal for Guidelines on information and communication technology (ICT) security and governance (Consultation deadline: 13th March 2020). Furthermore Austrian supervision focuses inter alia on effects of digitization in its activities for 2020 which means that operative measures and on site inspections will focus on IT security, IT infrastructures, cloud services, digital networks and cyber resilience.

ESMA is also working on a Guideline concerning the Outsourcing to Cloud Service Providers.

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

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

The answer provided is based on the Austrian Financial Market Authority's (FMA) and the Austrian National Bank's (OeNB) currently available perception of financial market participants operating in Austria:

Based on a national Cyber Maturity Level Assessment 2019 for the Insurance Sector (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]), it can be concluded that on average AT's insurance undertakings have taken material measures to ensure cyber security. In general, technical measures to strengthen insurance undertakings' cybersecurity, eg regarding IT-Assets, authorization concepts, network security, configurations & security setting or data security & encryption, outperform organizational ones, like the adoption of a cybersecurity strategy or the analyses of cybersecurity staff needs.

- For example, in general, inventories of hardware assets – and to a slightly lesser extent for software assets – are done automatically. Therefore the basis for the derivation of further security measures, especially for vulnerability and for patch management, is set.
- Most of AT's insurance undertakings also stick to the "need to know"-principle.
- Another example would be, that, in general, staff needs, job profiles and allocations of responsibilities don't specifically address cybersecurity issues, at the moment.

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

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

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

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

Austrian supervision of ICT risks is carried out by dedicated departments in FMA and OeNB. At this point there is no single designated department responsible for supervision of ICT risks. By applying an integrated supervisory approach, the departments are working closely together to ensure a common approach on ICT risk supervision. Furthermore there are several committees dealing with ICT-related questions.

The answer provided is based on the Austrian Financial Market Authority's (FMA) and the Austrian National Bank's (OeNB) currently available perception of financial market participants operating in Austria:

Regarding the Insurance Sector, Austria's Cyber Maturity Level Assessment 2019 (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]) shows that, in general, technical measures to strengthen insurance undertakings' cybersecurity, eg regarding IT-Assets, authorization concepts, network security, configurations & security setting or data security & encryption, outperform organizational ones, like the adoption of a cybersecurity strategy or the analyses of cybersecurity staff needs.

- For example, in general, inventories of hardware assets – and to a slightly lesser extent for software assets – are done automatically. Therefore the basis for the derivation of further security measures, especially for vulnerability and for patch management, is set.
- Most of AT's insurance undertakings also stick to the "need to know"-principle.
- Another example would be, that, in general, staff needs, job profiles and allocations of responsibilities don't specifically address cybersecurity issues, at the moment.

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

The yearly updated Supervisory Review and Evaluation Process (SREP) - Questionnaire includes questions regarding the implementation of the ICT risk management function in less significant credit institutions (LSI). The implementation of the information security officer is evaluated for each institution on a case by case basis. Regarding the Insurance Sector, Austria's Cyber Maturity Level Assessment 2019 (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]) shows that roughly three quarters of AT's insurance undertakings have established a chief information security officer (in different organisational units).

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

Type of arrangement, policy, measure	*Yes*	*No*	*Don't know/not applicable*
Do you establish and maintain updated a mapping of your organisation's business functions, roles and supporting processes?			x
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)?			x
Do you classify the identified business functions, supporting processes and information assets based on their criticality?			x
Do you map all access rights and credentials and do you use a strict role-based access policy?			x
Do you conduct a risk assessment before deploying new ICT technologies / models?			x
Other (please specify)			x

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

Austria's Cyber Maturity Level Assessment 2019 (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]) for the Insurance Sector shows that, in general, technical measures to strengthen insurance undertakings' cybersecurity, eg regarding IT-Assets, authorization concepts, network security, configurations & security setting or data security & encryption, outperform organizational ones, like the adoption of a cybersecurity strategy or the analyses of cybersecurity staff needs.

- For example, in general, inventories of hardware assets – and to a slightly lesser extent for software assets – are done automatically. Therefore the basis for the derivation of further security measures, especially for vulnerability and for patch management, is set.
- Most of AT's insurance undertakings also stick to the "need to know"-principle.
- Another example would be, that, in general, staff needs, job profiles and allocations of responsibilities don't specifically address cybersecurity issues, at the moment.

IT strategy and its related documents regarding the implementation, its evaluation as well as the internal control system of IT risks are part of the yearly updated SREP-Questionnaire of LSI – credit institutions. The arrangements, policies or measures are evaluated for each institution on a case by case basis.

Supervised Entities in the Securities Supervision should have in place an ICT and security risk management framework. In 2019 supervisory soft law has been published by FMA to create a common understanding of the expected level of ICT resilience (see: https://www.fma.gv.at/fma/fma-leitfaeden/). This framework should enable the companies to identify, detect and avoid or minimize ICT risks.

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

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

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

   Please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

Based on national supervisory experience gained in the course of collecting data on cyber events and incidents, we would like to note that a clear definition of „cyber-attack“ would have to be provided in Union law in order to allow for meaningful comparisons. Up to now, regarding AT's insurance undertakings and supervised entities in the Securities Supervision, no major cyber incidents have taken place.

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

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

   To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

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

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

Based on Austria's Cloud Maturity Level Assessment 2019 (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]) for the Insurance Sector, it can be concluded that almost one third of AT's cloud using insurance undertakings have already developed and established a separate cloud strategy. Based on a supervisory digitalization study of 2019 70 % of credit institutions, 20% of investment firms and 50% of Asset Managers in Austria use cloud-services.

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

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

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

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

    To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

According to our analyses the majority of credit institutions use legacy systems. In most cases appropriate mitigation measures have been taken.

Depending on the area of application, ICT systems have been in use for six to 16 years on average in AT's insurance undertakings, depending on the respective undertaking's situation.

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

problematic' and 5 for 'highly problematic').

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

The Austria's Cyber Maturity Level Assessment 2019 (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]) for the Insurance Sector shows that in general, technical measures to strengthen insurance undertakings' cybersecurity, eg regarding IT-Assets, authorization concepts, network security, configurations & security setting or data security & encryption, outperform organizational ones, like the adoption of a cybersecurity strategy or the analyses of cybersecurity staff needs.

- For example, in general, inventories of hardware assets – and to a slightly lesser extent for software assets – are done automatically. Therefore the basis for the derivation of further security measures, especially for vulnerability and for patch management, is set.
- Most of AT's insurance undertakings also stick to the "need to know"-principle.
- Another example would be, that, in general, staff needs, job profiles and allocations of responsibilities don't specifically address cybersecurity issues, at the moment.

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

- □ ~~*Yes*~~
- □ ~~*No*~~
- □ ~~*Don't know*~~*/Not Applicable*

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

Austria's Cyber Maturity Level Assessment 2019 (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]) for the Insurance Sector shows that requirements on encryption vary among AT's insurance undertakings. Overall, almost three quarters of AT's insurance undertakings have consistently implemented relevant standards.

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

- □ *Yes*
- □ ~~*No*~~
- □ ~~*Don't know/not Applicable*~~

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

Credit institutions are required to have a structured policy for ICT change management and regular patching and a detailed backup policy. When conducting on-site inspections this requirement can be reviewed.

Austria's Cyber Maturity Level Assessment 2019 (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]) for the Insurance Sector shows that almost three quarters of AT's insurance undertakings perform daily backups. Based on the same assessment, it can also be concluded that about two thirds of AT's insurance undertakings perform patches within a maximum of two weeks.

Supervised entities in the Securities Supervision are required to have a policy for ICT change management and regular patching and a backup policy. In 2019 supervisory soft law has been published by FMA to create a common understanding of the expected level of ICT resilience (see: https://www.fma.gv.at/fma/fma-mindeststandards/). When conduction on-site inspections this requirement can be reviewed.

15. Do you consider that your organisation has established and implemented security measures to

manage and mitigate ICT and security risks (e.g. organisation and governance, logical security, physical security, ICT operations security, security monitoring, information security reviews, assessment and testing, and/or information security training and awareness measures)?

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

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

Based on Austria's Cyber Maturity Level Assessment 2019 (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]) for the Insurance Sector, it can be concluded that on average material measures have been taken by AT's insurance undertakings to ensure cyber security.

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

    To the extent you deem it necessary, please specify and explain. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

Up to now, regarding AT's insurance undertakings, no major cyber incidents have taken place.

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

Issues	*Yes*	*No*	*Don't know/not applicable*
Lack of comprehensive business continuity policy and/or recovery plans			X
Difficulties to keep critical/ core business operations running and avoid shutting down completely			X

Internal coordination issues (i.e. within your organisation) in the effective deployment of business continuity and recovery measures			X
Lack of common contingency, response, resumption/recovery plans for cyber security scenarios - when more financial actors in your particular ecosystem are impacted			X
No ex-ante determination of the precise required capacities allowing the continuous availability of the system			X
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			X
Difficulty to isolate and disable affected information systems			X
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

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

    To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

Supervised Entities in Securities Supervision follow the common requirements in the relevant chapters of the FMA-Guideline on ICT Security (availability and continuity, emergency management, see: https://www.fma.gv.at/download.php?d=3597 [only available in German]).

RTO and RPO are both covered in Guideline 20 (Business continuity planning) and in Guideline 22 (Testing of plans) as well as in EIOPA's consultation paper on the proposal for Guidelines on Information and Communication Technology (ICT) security and governance. Austria participated in the drafting process of these Guidelines.

However, from an internal security perspective, RTO and RPO are viable instruments for fault- and error-based incidents and disasters. In case of cyber attacks, both could effectively be even counterproductive in nature. Given the fact that common best practice and industry standards strongly recommend analyzing attackers and motives to a certain extent before taking active steps to eliminate hostile intruders and their influence, instituting mandatory durations and objective could probably prevent state-of-the-art cyber defense and resilience procedures.

From an Oversight perspective, a set of mandatory key figures for RTO and RPO may not be comprehensive or conclusive enough for ensuring security evaluation. For Supervisor's work it would be better to gain access to detailed qualitative reports which enable critical analysis on a much deeper level of significance and information.

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

	Yes	*No*	*Don't know/not applicable*
Do you promote staff education on ICT and security risk through regular information sessions and/or trainings for employees?			x
Do you regularly organize dedicated trainings for the Board members and senior management?			x
Do you receive from the Board all the support you need for implementing effective cyber incident response and recovery improvement programs?			x
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?			x
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

Up to now, regarding AT's insurance undertakings as well as supervised entities in Securities Supervision, no major cyber incidents have taken place. Regarding cyber security awareness, Austria's Cyber Maturity Level Assessment 2019 (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]) for the Insurance Sector shows that almost three quarters of AT's insurance undertakings are taking material measures to increase cyber security awareness of their stakeholders by communicating the aims and the focus of their respective cyber security strategy.

2.2. ICT and security incident reporting requirements

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

Questions:

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

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

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

- □ *Yes*
- □ ~~*No*~~

□ ~~*Don't know*~~

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Since all financial institutions are closely interconnected and often face threats of similar nature, a harmonized EU-wide methodology and system for ICT incident reporting would be advisable.

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

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

A comprehensive and harmonised EU-wide ICT incident reporting framework would unburden financial market participants (FMP) and would lead to a cross sectoral level playing field. It is expected that uniform reporting standards improve incident data consistency as well as providing actual comparable data of ICT incidents. Authorities in Austria are tasked with cross-sectoral prudential supervision, the Financial Market Authority as well as Oesterreichische Nationalbank (OeNB) therefore have in-depth experience with reporting regimes for FMP. One of the main goals of Austrian supervision is to overcome the silo approach in reporting as well as enabling the “file only once” principle. Especially the taxonomy and materiality thresholds are key in our opinion in order to ensure a high level of data quality, integrity and coherence. Currently FMP (note: this is not the case for insurance undertakings) must report ICT incidents due to sectoral legislation in an unharmonised granularity, at different points in time and through different reporting channels. Harmonised reporting timetables and forms would lessen the burden for FMP while still maintaining a high level of cyber incident awareness in the EU. A harmonised ICT incident reporting regime should take the risks associated with the specific type of FMP into account and needs to address these in a proportional matter.

Therefore, in general as much harmonisation as possible would be welcomed. However, divergent legal bases, eg regarding reporting timeframes, should also be considered. On top of this, deviating sector specific information security priorities (e.g., availability seems to be of higher immediate relevance in the Banking Sector than in the Insurance Sector or the Securities Sector) could play a role in the process of drawing up incident reporting requirements. Also, materiality thresholds are generally useful reporting items, but definitely need precise definition (eg: thresholds for incidents, thresholds for institute).

For credit institutions there are several incident reporting frameworks in place. A harmonized EU-wide ICT incident reporting framework should cover (and thus replace) all existing frameworks (ie incident reporting according to PSD 2, ECB framework for major incidents for SI, reporting according to NIS-Directive).

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

    To the extent you deem it necessary, please explain your reasoning. [Insert text box]

There are several reporting frameworks in place for credit institutions (see question 22). The level of detail and the information required in these existing reports should be reviewed when designing a new framework (The level of detail required by the ECB Cyber Incident Reporting Framework should be sufficiently granular for supervisory work. EBA Guidelines on major incidents reporting under PSD2 are good guidance to a minimum level of reporting detail. Input could also be asked from EBA TFIT and/or the ECB IT expert group.). The Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector (JC/2019/26) contains a common vision for an improved European ICT risk management framework.

At the moment, an EIOPA project group is also engaged with these questions. Austria is taking part in this work.

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

    □ ~~*Yes*~~

    □ *No*

    □ ~~*Don't know*~~

    To the extent you deem it necessary, please explain your reasoning. [Insert text box]

It must be stressed that materiality thresholds are a necessity for efficient, fundamental supervisory work. Without a comprehensive set of thresholds, supervisors are confronted with an excessive and possibly unmanageable amount of data. Also, thresholds should not be limited to monetary ranges but could also comprise of other qualitative key indicators which seem meaningful to authorities. Development of such key indicators should be subject of debate between supervisors, beforehands.

Materiality thresholds are the logical conclusion if a proportional approach to cyber incident reporting is applied. Furthermore financial market legislation should always strive to limit the additional burden for financial market participants (FMP) where possible, the reporting of every cyber incident would create a disproportionate effort for FMP. As public authority tasked with the prudential supervision of FMP our experience is, that the success of materiality thresholds is linked directly to the clarity of their definition. Unless defined well, FMP will interpret materiality thresholds differently which leads to skewed data and incomparability. Due to this reasons we generally advise to include materiality thresholds in a potential European cyber incident reporting framework and point out that the clarity and definition of the materiality thresholds is key to enable a level playing field and prevent arbitrary reporting.

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

    To the extent you deem it necessary, please explain your reasoning. [Insert text box]

As ICT incidents may occur at any time and legislation regularly demands financial market participants (FMP) to report them promptly, a competent authority would ideally have resources to process incident reports twenty-four hours a day and seven days per week. Furthermore, technical expertise is needed to assess reported ICT incident and to offer guidance for public authorities as well as FMP.

Report recipients should be based on the respective purposes of the reports. But, as far as possible, entities should not be obliged to submit reports to more than one recipient. From a supervisory point of view, it is important to receive incident reports due to supervisory needs.

A single and clear reporting chain is of central importance for efficient and encompassing incident reporting. Coordination should most probably be concentrated in the hands of one competent European information hub or authority (eg: ECB, EBA), capable of constantly monitoring and conveying the full landscape of threats and incidents. The scope of reporting requirements should be proportionate.

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

- □ *Yes*
- □ ~~*No*~~
- □ ~~*Don't know*~~

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Integrated financial supervision is tasked with the cross sectoral supervision of financial market participants (FMP). In our experience a high percentage of FMPs is operating cross-border, therefore a standing mechanism to exchange incident reports is needed to address ICT risks appropriately. In analogy to national CERT information sharing or standing mechanisms of the ECB in the area of payment system oversight, (anonymized) reports should definitely be shared among competent authorities on all levels (eg: as early warning indicator, for benchmarking reasons).

However, a thorough analysis of the possibilities regarding the exchange of data on incident reports, also taking into account the role of the ESAs, should be conducted before the implementation of such a mechanism.

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

To the extent you deem it necessary, please explain your reasoning and provide concrete examples. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

At the moment, EU confidentiality requirements are not ideal for the sharing of sensible data and information (GDPR being one of the main obstacles, for instance) and are a major obstacle for cross-border cooperation as well as for cooperation within the national financial sector.

From the companies' viewpoint, leakage of potentially compromising information and reputational concerns may also be barriers to transparency and openness.

2.3. Digital operational resilience testing framework

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

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

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

Questions:

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

- □ ~~*Yes*~~
- □ ~~*No*~~
- □ ~~*Don't know*~~*/not applicable*

If the answer is yes:

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

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

Do you face any issues with overlapping or diverging obligations?			
Do you practice ICT and security testing on a voluntary basis?			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

The ESAs published the Joint Advice for the development of a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole financial sector (see: https://www.eiopa.europa.eu/content/esas-publish-joint-advice-information-and-communication-technology-risk-management-and_en). The application of a coherent cyber resilience testing framework should be proportionate to the type, size and business model of a relevant entity. Austria supports this approach.

Credit institutions currently do face overlapping regulation, especially regarding incident reporting.

Austrian supervision developed a Cyber & Cloud Maturity Level Assessment (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]). In 2019, AT's insurance undertakings subject to Solvency II took part in both assessments, while AT's Pension Sector participated in the Cloud Maturity Level Assessment.

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

Different elements of a baseline testing/assessment framework	*Yes*	*No*	*Don't know/ not applicable*
Gap analyses?	x		
Compliance reviews?	x		
Vulnerability scans?	x		
Physical security reviews?	x		
Source code reviews?		x	
Others (please specify)			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Austrian supervision (FMA in cooperation with OeNB and BMF) published soft law instruments on ICT risk for all supervised sectors. Our expectation as public supervisory authority is that financial market participants (FMP) have risk management processes in place to address their cyber risks adequately. Generally, FMP are not tasked to implement specific ICT measures unless European or national legislation demands otherwise. From a supervisory standpoint FMP are free to choose their preferred methods as long as an appropriate level of cyber resilience is ultimately achieved. We do see merit in all methods mentioned above for baseline testing except source code reviews as these are usually too resource intensive if done properly for baseline testing and therefore currently disproportionate. Proportionality should be a key component of the European testing framework to address risks in an adequate matter without overburdening FMP. Although if technology allows for greater flexibility and easier testing (eg: AI assisted code review), than even currently disproportionate methods can become sensible over time.

Based on EIOPA's proposal for Guidelines on Information and Communication Technology security and governance (see: https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-information-and-communication-technology-security-and-governance_en), insurance undertakings should perform a variety of different information security reviews, assessments and testing, so as to ensure effective identification of vulnerabilities in its ICT systems and services. On top of this, tests should include vulnerability scans and penetration tests.

Credit institutions are already required to do at least some of the above according to the GL on ICT and security risk management (see: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management).

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

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

It seems reasonable to apply advanced testing to operators of essential services according to Art. 4 para. 4 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS-Directive). For the purposes of Art. 4 NIS-Directive, differentiation criteria for banking and financial market infrastructure institutions are listed in Annex II to determine operators of essential services. These operators have already been identified across the European Union and are a suitable starting point for increased cyber resilience testing candidates among financial market participants. The national transposition of the NIS-Directive has been achieved by changing existing (e.g. Payment Services Act, ZaDiG 2018) as well as introducing new legislative acts (e.g. Security of Network and Information Systems Act, NISG, and the Security of Network and Information Regulation, NISV, which specifies the NISG).

For the **banking sector** (§ 6 NISV), the NISV has a **purely clarifying function**, since the provisions of the ZaDiG 2018, on operational and security-related risks (§§ 85 and 86 ZaDiG 2018), take precedence over the provisions of the NISG (§ 20 para. 1 NISG, § 6 para. 3 NISV). The banking sector in Austria is only covered by the NISG so that banks may also be able to establish a separate sectoral CERT. According the national transposition of the NISG, national supervision is obliged to pass on major operating or security incidents pursuant to Article 86 ZaDiG 2018 that have happened at the operators of material services in the sector for the banking system to the Federal Minister for the the Interior without delay (Article 20 para. 2 NISG). Thus, double reporting is avoided, one filing is sufficient.

Generally all of the listed perspectives should be considered. For financial entities (eg: credit institutions) comprehensive, SSM-wide classification systems (eg: significant credit institutions [SI], less significant credit institutions [LSI]; high priority LSI [HP-LSI], medium priority LSI [MP-LSI], low priority LSI [LP-LSI], systematically important payment systems [SIPS], prominently important retail payment systems [PIRPS], other retail payment systems [ORPS]) have already been implemented by the ECB which can be used accordingly for ICT- and incident-based purposes. there is already a classification between SI, HP-LSI, MP-LSI and LP LSI that could be used in this regard.

It would also make sense for the operators of data centres which provide services for financial market participants to be recognised as operators of material services as defined in the NISG, since operational or security incidents predominantly become apparent at such facilities directly, and only subsequently at the entities that they in turn service.

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

	Yes	*No*	*Don't know/ not applicable*
Should it be run on all functions?			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			x
held validfor 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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

At this point in time it is not possible to fully assess the proper scope for advanced testing and it should definitely not be a mandatory requirement of any kind but both company and circumstances specific. A focus could be set on live production testing. Certified or dedicated testers would be highly welcome and a sign of good practice. Certifications should be selected from existing best practices and not create personnel shortage among available testers.

Currently there are several initiatives on the European level, their outcome should enable European legislators to take an informed decision on the needed scope. Based on the lessons learned, eg by EIOPA's Threat Lead Penetration Testing (TLPT) pilot project (see: EIOPA's Supervisory Convergence Plan for 2020, section supervision of emerging risks, https://www.eiopa.europa.eu/sites/default/files/publications/supervisory-convergence-plan-for-2020.pdf) above questions could be answered. Furthermore the European framework for threat intelligence-based ethical red-teaming (TIBER-EU, see: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html) could be a solution. However, since it is very extensive, there would be the need to design different application models.

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

- □ ~~*Every six months*~~
- □ ~~*Every year*~~
- □ ~~*Once every three years*~~
- □ *Other [Insert text box]*

See text box below

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

The appropriate testing frequency mainly depends on the risk assessment and the resources needed to perform the testing if a proportional approach is applied to cyber resilience testing. Resource intensive advanced testing methods should be performed less frequently or only on a case-by-case basis if there is a specific supervisory need to do so. European legislation on the frequency of advanced testing needs therefore to take the costs and resources needed for advanced testing on the one hand and on the other hand the size of financial market participants, which are subject to advanced testing, into account.

A general statement about the appropriate testing frequency is therefore not finally possible. That being said, advanced testing methods like Threat Lead Penetration Testing (TLPT) are quite cost-intensive, an obligatory frequency of less than two years seems disproportionate, at first view. A frequency of two years could be appropriate for many ICT systems (in relation to the timespan necessary for implementing changes and improvements). A period of one year or below seems inappropriate in most cases.

In any case, individual frequency requirements should be subject to proportionality aspects. A requirement to perform advanced testing is a sufficient cyber maturity levels of the tested financial entities. Due to this reason the Austrian supervision developed and implemented a Cyber & Cloud Maturity Level Assessment (see: *FMA Facts & Figures 2020* section "How digital is Austria's financial market?" subsection "The FMA's new Benchmark for companies' approach to cybersecurity", https://www.fma.gv.at/download.php?d=4245 as well as *Bericht der FMA 2019 zur Lage der österreichischen Versicherungswirtschaft* [FMA Report 2019 regarding Austria's Insurance Sector] section "Technologisches Umfeld" [Technological Environment], https://www.fma.gv.at/download.php?d=4252 [unfortunately only available in German]).

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

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Austrian supervision published in 2018 soft law instruments (see: https://www.fma.gv.at/fma/fma-mindeststandards/) on ICT security for financial market participants (FMP) to communicate transparently FMA's expectations and to create a common understanding about the needed level of cyber resilience in the financial market sector. Moreover, cyber resilience is part of the audit and supervisory focuses for 2020. European legislation regarding baseline testing and advanced testing methods has the potential to harmonise cyber resilience testing across the financial market sector and address cyber threats in a proportional, risk-based and coherent approach across the currently fragmented sectoral legislation.

In our view, both versions could have a prudential impact.

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

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

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

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

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

Questions:

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

The supervisory authorities are currently gathering information about ICT third party provider used by market participants. The supervisory analysis includes a screening for concentration risks linked to the usage of ICT third party providers.

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

    - □ ~~*Yes*~~
    - □ ~~*No*~~
    - □ ~~*Don't know*~~*/not applicable*

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

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

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

    To the extent you deem it necessary, please explain your reasoning [Insert text box]

On a technical level, the implementation of standard contractual clauses has been considered in the EBA working group that elaborated the GL on Outsourcing but it was found that such clauses would have to be updated regularly as technology continues to develop. Furthermore, it is questionable whether such clauses could be designed to fit all possible cases.

In principle, it should be noted that many current requirements required by guidelines and other legal bases cannot be demanded by small market participants from large cloud service providers (CSP). Due to the market power of the CSP, a kind of standard contract should be drawn up at European level that covers the required standards. At European level, possible areas for contractual requirements could include audit rights and classification of information sensibility (the term “audit rights” includes both internal audit as well as supervisory examinations).

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

	Yes	*No*	*Don't know/not applicable*
Should an oversight framework be established?	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 nonbinding tools (e.g. recommendations, crossborder 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		

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

ICT third party providers are nowadays essential for many business processes of financial market participants (FMP). The reliance on external infrastructure and services on the one hand and on the other hand the risks involved in outsourcing generally, create a need for supervision to address these risks adequately. Furthermore, leading ICT third party providers in the financial market sector pose a potential concentration risk, which needs to be managed properly. Austria's point of view is that contractual clauses in outsourcing agreements alone are not sufficient to address the risks linked to ICT third party providers in the financial market sector. Thus European legislation, which introduces an oversight framework for ICT third party providers is seen as a needed step to mitigate the risks associated with outsourcing and reliance of FMP on ICT third party providers. Limiting the supervision to non-binding instruments is seen as inadequate by Financial Market Authority, whereas the National Bank would see non-binding instruments in case of payment systems oversight as sufficient.

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

	Yes	*No*	*Don't know/not applicable*
Diversification strategies, including a potential mandatory or voluntary rotation mechanism with associated rules to ensure portability (e.g. auditing model)	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		
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

The supervisory authorities are currently gathering information about ICT third party provider used by market participants. This provides the basis for considering the most appropriate and effective solutions to address potential concentration risks.

Diversification is a good instrument, but a mandatory multi-provider approach seems too restrictive. As credit institutions have to notify their supervisor of all significant outsourcing arrangements, we have a possibility to take measures if an outsourcing arrangement seems inappropriate regarding concentration risks.

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.

Questions:

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

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

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

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

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

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

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions. As such we are also backing the respective work performed by the ESAs, though.

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

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

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

Generally speaking, major challenges exist regarding to GDPR and legitimacy of sharing of data within the EU. Besides legal issues, concerns may also exist due to various aspects of information leakage and thus reputational considerations.

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems and reporting methods of supervisory institutions.

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

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

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

Generally, Austrian supervision sees an improved level of information sharing across different jurisdictions as positive. Creating more awareness for cyber threats improves the understanding of supervisory authorities and financial market participants (FMP) for the specific cyber resilience needs of the financial market sector. As risks linked to the use of ICT are changing very dynamically, it is important to stay informed on the current cyber threats as outdated risk assessments may erode an entities cyber resilience. Also, sharing of information on cyber incidents would be vital for building effective, common threat awareness and response mechanisms.

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

Questions:

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

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

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

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions. Therefore questions about a potential institutional cyber insurance would be beyond the scope of this consultation.

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

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

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions. Therefore questions about a potential institutional cyber insurance would be beyond the scope of this consultation.

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

Issues	*Yes*	*No*	*Don't know/not applicable*
Lack of a common taxonomy on cyber incidents	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		
Other (please specify)			

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

The cyber insurance market is currently fairly opaque. For one, there are substantial differences in the definitions of what cyber insurance actually is. Moreover, the range of products and services in this segment is relatively heterogeneous.

When deciding whether to offer cyber insurance products, providers face the conundrum of seizing a first mover advantage to quickly gain market share vs. the need for risk-adequate premium calculation. Statistical experience and data are still sparse due to the high number of unreported cases of damage caused by cyber risks. The environment is also constantly changing. Appropriate premium calculation is therefore challenging, and the risk of underpricing should not be underestimated.

Regarding taxonomy, there are viable proposals by European initiatives (eg: ESRB's European Systemic Cyber Group taxonomy and classifications on Systemic Cyber Risk) which could be useful for developing risk transfer and mitigation mechanisms.

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

□ *Yes*

□ ~~*No*~~

□ ~~*Don't know/no opinion*~~

To the extent you deem it necessary, please explain your reasoning. [Insert text box]

The respective work of the ESAs is backed by Austria.

2.6. Interaction with the NIS Directive

The NIS Directive is the first internal market instrument aimed at improving the resilience of the EU against cybersecurity risks. Although it has a broad scope (covering different economic areas), as far as the financial services are concerned, only entities belonging to three financial services sectors (credit institutions, operators of trading venues, central counterparties) are covered. Entities from other financial sectors services (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 NIS. Their relevant ICT and security risk requirements remain covered by their specific pieces of legislation. Even for the three abovementioned financial sectors which the NIS Directive covers, the *lex specialis* clause allows the Directive not to be applied whenever EU sector specific legislation has at least equivalent requirements[15].

Even when the NIS Directive applies to three types of financial services entities this does not mean that all entities active in those sectors are necessarily covered. The co-legislators have delegated the precise scope of application of the NIS Directive to the Member States which need to a) identify operators of essential services and b) establish a list of services - which are essential for the maintenance of critical societal and /or economic activities (one criteria in the process of

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

identification of operators of essential services). Member States may identify additional services which they deem to be essential. The identification of 'operators providing essential services' is based on three criteria spelled out in the NIS. The NIS Directive is also a minimum harmonization *directive.*

Questions:

47. 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*~~

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

The national transposition of the NIS-Directive has been achieved by changing existing (e.g. Payment Services Act, ZaDiG 2018) as well as introducing new legislative acts (e.g. Security of Network and Information Systems Act, NISG, and the Security of Network and Information Regulation, NISV, which specifies the NISG). For the **banking sector** (§ 6 NISV), the NISV has a **purely clarifying function**, since the provisions of the ZaDiG 2018, on operational and security-related risks (§§ 85 and 86 ZaDiG 2018), take precedence over the provisions of the NISG (§ 20 (1) NISG, § 6(3) NISV).

The banking sector in Austria is only covered by the NISG so that banks may also be able to establish a separate sectoral CERT.

According to the national transposition of the NISG, Austria's Financial Market Authority is obliged to pass on major operating or security incidents pursuant to Article 86 ZaDiG 2018 that have happened at the operators of material services in the sector for the banking system to the Federal Minister for the Interior without delay (Article 20 para. 2 NISG).

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. [Insert text box]

The answer provided is based on the Austrian Financial Market Authority's (FMA) and the Austrian National Bank's (OeNB) currently available perception of financial market participants operating in Austria:

In Austria significant credit institutions and the market infrastructures are operators of essential services and are therefore in the scope of the NIS-Directive.

The national transposition of the NIS-Directive has been achieved by changing existing (e.g. Payment Services Act, ZaDiG 2018) as well as introducing new legislative acts (e.g. Security of Network and Information Systems Act, NISG, and the Security of Network and Information Regulation, NISV, which specifies the NISG).

For the **banking sector** (§ 6 NISV), the NISV has a **purely clarifying function**, since the provisions of the ZaDiG 2018, on operational and security-related risks (§§ 85 and 86 ZaDiG 2018), take precedence over the provisions of the NISG (§ 20 (1) NISG, § 6(3) NISV). § 6 NISV stipulates what constitutes essential services for the institutions concerned (these are exclusively services related to payment transactions) and what has to be qualified as a security incident according to the NISG. However, the thresholds stipulated in § 6 NISV are of little relevance, as the criteria under **§ 86 ZaDiG 2018** (**serious operational or security incidents**) and the EBA Guidelines on Major Incidents Reporting are much stricter. For this reason, reporting obligations to the supervision are triggered for institutions, even if the thresholds in § 6(2) NISV are not met. In this context, supervisors will in the future be **obliged to immediately report all serious operational or security incidents pursuant to § 86 ZaDiG 2018 that have occurred at credit institutions (identified as operators of essential services) to the Federal Minister of the Interior (§ 20(2) NISG).** It should be noted that only CRR credit institutions, superordinate credit institutions or central organisation of a network of credit institutions whose total assets exceed EUR 30 billion may be identified as operators of essential services in the banking sector.

For the **financial market infrastructure sector**, §7(3) NISV stipulates that the BörseG 2018, EMIR and CSDR or the relevant Regulatory Technical Standards (RTS) contain **provisions** that ensure at least an **equivalent level of security** for network and information systems pursuant to §20 NISG. Thus, the provisions on security measures (§ 17 NISG) are not applicable to financial market infrastructures. However, the reporting **obligations according to § 19 NISG are applicable**, since the above-mentioned sectoral regulations have not been determined as equivalent.

AT's insurance sector is not covered in the NIS-scope.

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

To the extent you deem it necessary, please explain your reasoning and provide details. [Insert text box]

Answers provided are based on a purely supervisory view and hence its institutions are beyond the regulatory remit of financial service legislation.

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

50. *Did you encounter 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. [Insert text box]

Not applicable

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

    Please provide details on your experience. [Insert text box]

Not applicable

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

52. *Do you receive NIS relevant information in relation to a financial entity under your remit? Please detail your experience, specifying how this information is shared (e.g. ad hoc, upon request, regularly) and providing any information that may be disclosed and you consider to be relevant. [Insert text box]*

The national transposition of the NIS-Directive has been achieved by changing existing (e.g. Payment Services Act, ZaDiG 2018) as well as introducing new legislative acts (e.g. Security of Network and Information Systems Act, NISG, and the Security of Network and Information Regulation, NISV, which specifies the NISG). For the **banking sector** (§ 6 NISV), the NISV has a **purely clarifying function**, since the provisions of the ZaDiG 2018, on operational and security-related risks (§§ 85 and 86 ZaDiG 2018), take precedence over the provisions of the NISG (§ 20 (1) NISG, § 6(3) NISV).

The banking sector in Austria is only covered by the NISG so that banks may also be able to establish a separate sectoral CERT.

According to the national transposition of the NISG, Austria's Financial Market Authority is obliged to pass on major operating or security incidents pursuant to Article 86 ZaDiG 2018 that have happened at the operators of material services in the sector for the banking system to the Federal Minister for the Interior without delay (Article 20 para. 2 NISG).

On the basis of Article 86 ZaDiG 2018 (Payment Services Act, ZaDiG 2018) all supervised institutions within the banking sector are obliged to report major operational or security incidents (within the prescribed timeframes, in the EBA GL on major incident reporting) to OeNB and FMA. This information must then be forwarded to EBA without delay and under certain conditions also to other national and international authorities (e.g. the BMI (Federal Ministry for the Interior), the BKA (Bundeskriminalamt, Criminal Information Service Austria, and the BVT (Federal Agency for State Protection and Counter Terrorism). It is necessary to forward the reports to another national or international authority, where the incident falls within the scope of their competence, or if the incident attracts wide-scale media attention (see the EBA GL on major incident reporting). An obligation for Austrian Supervision to forward such reports also exists in accordance with Article 20 para. 2 NISG (Security of Network and Information Systems Act, NISG) to the Federal Minister of the Interior.

AT's insurance sector is not covered in the NIS-scope.

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

    Please explain your reasoning [Insert text box]

A clear framework for ICT and security risk management is necessary to have a level playing field across the financial sector. NCAs and NCBs should be entrusted accordingly with this task (eg: prudential, oversight, conduct/governance).

Austrian Supervision is already responsible to a certain extent for the supervision of ICT and security risks for the banking sector (Articles 85 and 86 Payment Services Act, ZaDiG 2018, and EBA GL on ICT and Security Risk Management).

Synonymous to other areas of supervision, Austria backs the aim to harmonize supervisory activities.

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

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

If you answered yes, please explain those particular issues. [Insert text box]

We have not encountered difficulties in obtaining information yet. AT's insurance sector is not covered in the NIS-scope.)

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

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

If you answered yes, please explain which issues. [Insert text box]

The major incident reporting for SI introduced by ECB for SI foresees international cooperation and coordination. For LSI there is currently no such framework.

To date no severe operational or security incident has occurred that affect another national or international supervisory authority. The forwarding of reports to supervisory authorities functions smoothly.

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. [Insert text box]

We have satisfying experience with the lex specialis clause. Helpful applications of the clause exist in the areas of NIS reporting and PSD2, as well as in smooth and fluent cooperation between competent authorities.

The national transposition of the NIS-Directive has been achieved by changing existing (e.g. Payment Services Act, ZaDiG 2018) as well as introducing new legislative acts (e.g. Security of Network and Information Systems Act, NISG, and the Security of Network and Information Regulation, NISV, which specifies the NISG).

For the **banking sector** (§ 6 NISV), the NISV has a **purely clarifying function**, since the provisions of the ZaDiG 2018, on operational and security-related risks (§§ 85 and 86 ZaDiG 2018), take precedence over the provisions of the NISG (§ 20 (1) NISG, § 6(3) NISV). § 6 NISV stipulates what constitutes essential services for the institutions concerned (these are exclusively services related to payment transactions) and what has to be qualified as a security incident according to the NISG. However, the thresholds stipulated in § 6 NISV are of little relevance, as the criteria under **§ 86 ZaDiG 2018** (**serious operational or security incidents**) and the EBA Guidelines on Major Incidents Reporting are much stricter. For this reason, reporting obligations to supervisory authorities are triggered for institutions, even if the thresholds in § 6(2) NISV are not met. In this context, supervision in Austria will in the future be **obliged to immediately report all serious operational or security incidents pursuant to § 86 ZaDiG 2018 that have occurred at credit institutions (identified as operators of essential services) to the Federal Minister of the Interior (§ 20(2) NISG).** It should be noted that only CRR credit institutions, superordinate credit institutions or central organisation of a network of credit institutions whose total assets exceed EUR 30 billion may be identified as operators of essential services in the banking sector.

For the **financial market infrastructure sector**, §7(3) NISV stipulates that the BörseG 2018, EMIR and CSDR or the relevant Regulatory Technical Standards (RTS) contain **provisions** that ensure at least an **equivalent level of security** for network and information systems pursuant to §20 NISG. Thus, the provisions on security measures (§ 17 NISG) are not applicable to financial market infrastructures. However, the reporting **obligations according to § 19 NISG are applicable**, since the above-mentioned sectoral regulations have not been determined as equivalent.

3. POTENTIAL IMPACTS

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

Questions:

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

    Please provide details. [Insert text box]

Overall, trust in a secure digital environment will be increased, strengthening economic, social, corporate and development perspectives.

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

    Please provide details. [Insert text box]

All building blocks are of relevance.

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

    Please provide details. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

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

    Please provide details. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

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

    Please provide details. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.

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

Please provide details. [Insert text box]

Answers provided are based on a purely supervisory view and hence they do not include any operational issues regarding ICT systems of supervisory institutions.