Questions	Answers
Information about the respondent	
A. Name of respondent institution/firm	Austrian Financial Market Authority
B. Name of representative individual submitting response	Click here to enter text.
C. Email address of representative individual submitting response	joanna.rakowska@fma.gv.at
D. Do you request non-publication of any part(s) of this response? If so, which part(s)? *Unless non-publication (in part or whole) is specifically requested, all consultation responses will be published in full on the FSB's website. An automated e-mail confidentiality claim will not suffice for these purposes.*	Click here to enter text.
E. Would you like your response to be confidential (i.e. not posted on the FSB website)?	Choose an item.

Questions	Answers
Consultation questions	
General questions	
1. Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?	The COVID-19-pandemic illustrates that it is important for supervisory authorities to have a current overview over major cyber incidents as the significance of digital communication has further increased.
2. To whom do you think this document should be addressed within your organisation?	Cyber security is of interest for all FMA Departments. As the FMA is established for the purpose of conducting banking supervision, insurance supervision, securities supervision, and pension funds supervision, this document is especially relevant regarding the FMA's supervisory measures. Of course, it also applies to FMA's own cyber security and therefore it is also relevant for FMA's IT-related issues.
3. How does your organisation link cyber incident response and recovery with the organisation's business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks?	In 2019, the FMA performed a cyber maturity level assessment for the insurance sector (please refer to 'Bericht über die Lage der österreichischen Versicherungswirtschaft 2019', https://www.fma.gv.at/download.php?d=4341). In the course of this assessment, also cyber incidents had to be indicated by the undertakings. Based on the surveyed data, an interrelation between an undertaking's cyber maturity level and losses suffered due to cyber incidents can be assumed - a lower cyber maturity level might come along with higher losses due to cyber incidents. However, the data basis was too small to come up with a general assumption. Approximately three fourths of Austrian's insurance undertakings explicitly consider standards (eg ISO 2700x-standards or NIST).
4. Does your organisation structure its cyber incident response and recovery activities along the seven	FMA's cyber maturity level assessment for the insurance sector was not explicitly structured along these seven components.

Questions	Answers
components set out in the FSB toolkit? Please describe any additional components your organisation considers.	
5. Based on your organisation's experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s).	-
6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).	-
7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?	Increasing risk awareness, providing adequate respective requirements, ongoing dialogues with supervised financial undertakings are some examples regarding FMA's tasks.
1. Governance	
1.1 To what extent does your organisation designate roles and responsibilities as described in Tool 3? Does your organisation identify these roles by business line, technology application or department?	Solvency II requirements comprise governance specifications. On top of this EIOPA Guidelines on Information and Communication Technology (ICT) security and governance were already consulted.
1.2 How does your organisation promote a non-punitive culture to avoid "too little too late" failures and accelerate information sharing and CIRR activities?	The EIOPA Guidelines on Information and Communication Technology (ICT) security and governance also comprise requirements on ICT incident and problem management. Furthermore, e.g. the information security policy is to be communicated within the undertaking.

	Questions	Answers
2.	**Preparation**	
2.1	What tools and processes does your organisation have to deploy during the first days of a cyber incident?	Please refer to EIOPA Guidelines on Information and Communication Technology (ICT) security and governance, GL on ICT incident and problem management. Actual implementation in the supervised insurance undertakings is undertaking-specific.
2.2	Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.	Based e.g. on FMA's survey on cyber incidents or on FMA's digitalisation study (https://www.fma.gv.at/en/publications/study-on-digitalisation-of-the-financial-market/) and on the consulted EIOPA Guidelines on Information and Communication Technology (ICT) security and governance, it can be assumed that also cyber incident response plans have been enhanced in supervised insurance undertakings.
2.3	How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?	Service providers are also covered e.g. by the consulted EIOPA Guidelines on Information and Communication Technology (ICT) security and governance and were also covered by FMA's cyber maturity level assessment. The actual implementation is undertaking-specific.
3.	**Analysis**	
3.1	Could you share your organisation's cyber incident analysis taxonomy and severity framework?	The drawing up of EIOPA's incident reporting requirements are also going to play an important role respective insurance undertakings' cyber incident analysis taxonomy and severity framework.
3.2	What are the inputs that would be required to facilitate the analysis of a cyber incident?	In any case, cyber incident data is expected to also enable the measurement of ICT and security risk (from a supervisory view).
3.3	What additional tools could be useful to analyse the effectiveness of cyber incident response and recovery activities and the severity, impact and root cause of cyber incidents?	-

Questions	Answers
3.4 What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?	EIOPA Guidelines on Information and Communication Technology (ICT) security and governance require the supervised insurance undertakings to provide timely information, including incident reporting, to external parties, as appropriate and in line with an applicable regulation.
4. Mitigation	
4.1 Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?	Examples would be – inter alia – enabling timely recovery, effective communication and identification of root causes.
4.2 What tools or effective practices does your organisation have related to mitigating the impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events?	Answer is undertaking-specific.
4.3 What tools or practices are effective for integrating the mitigation efforts of third-party service providers with the mitigation efforts of the organisation?	Answer is undertaking-specific; however, ongoing communication is a basic requirement.
4.4 What additional tools could be useful for including in the component Mitigation?	-
4.5 Are there situations in which effective practices for mitigation and restoration activities of the organisation are the same or overlap substantially? If yes, please provide examples.	-
5. Restoration	
5.1 What tools and processes does your organisation have available for restoration?	Answer is undertaking-specific.
5.2 Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?	Answer is undertaking-specific.

Questions	Answers
5.3 How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?	Answer is undertaking-specific.
6. Improvement	
6.1 What are the most effective types of exercises, drills and tests? Why are they considered effective?	In any case, various reviews should be performed on a regular basis.
6.2 What are the major impediments to establishing cross-sectoral and cross-border exercises?	Major impediments would include considerations on data protection. Also, sector-specificities are to be taken into consideration. E.g. availability seems more important for the banking sector than for insurance undertakings, in general. On top of this, the respective cyber maturity levels and the significance of financial institutions should be taken into consideration, e.g. regarding the adequate exercise method.
6.3 Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?	Answer is undertaking-specific.
7. Coordination and Communication	
7.1 Does your organisation distinguish "coordination activities" from broader "communication" in general? If yes, please describe the distinct nature of each component.	E.g., in the EIOPA Guidelines on Information and Communication Technology (ICT) security and governance, communication plans are referred to separately.
7.2 How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?	Answer is undertaking-specific.
7.3 Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?	Incident reporting templates for insurance undertakings are currently drawn up by EIOPA.

Questions	Answers
	Other useful information could also be shared in the course of bilateral talks.