European Insurance and Occupational Pensions Authority

Comments to the "Discussion Paper on Methodological Principles of Insurance Stress Testing – Cyber Component"	**24 November 2022**

Responding to this paper

EIOPA welcomes comments on the "Discussion Paper on Methodological Principles of Insurance Stress Testing – Cyber Component".
Comments are most helpful if they:

- respond to the question stated, where applicable;
- contain a clear rationale; and
- describe any alternatives EIOPA should consider.

Please send your comments to EIOPA in the provided Template for Comments, by email to <**eiopa.stress.test@eiopa.europa.eu**> by **28 February 2023**. Contributions not provided in the template for comments, or sent to a different email address, or after the deadline will not be considered.

Publication of responses

Contributions received will be published on EIOPA's public website unless you request otherwise in the respective field in the template for comments. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure.
Please note that EIOPA is subject to Regulation (EC) No 1049/2001 regarding public access to documents[1] and EIOPA's rules on public access to documents[2]. Contributions will be made available at the end of the public consultation period.

Data protection

Please note that personal contact details (such as name of individuals, email addresses and phone numbers) will not be published. They will only be used to request clarifications if necessary on the information supplied. EIOPA, as a European Authority, will process any personal data in line with Regulation (EU) 2018/1725[3] on the protection of the individuals with regards to the processing of personal data by the Union institutions and bodies and on the free movement of such data. More information on data protection can be found at https://eiopa.europa.eu/ under the heading 'Legal notice'.

[1] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

[2] Public Access to Documents (See link: https://eiopa.europa.eu/Pages/SearchResults.aspx?k=filename:Public-Access - (EIOPA-MB-11-051).pdf).

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Reference	
Name of the Stakeholder	Institute and Faculty of Actuaries
Type of Stakeholder (please delete in the column to the right the categories which do not apply)	Association
Contact Person	Matthew Levine
Email address	Matthew.levine@actuaries.org.uk
Phone number	+44 7525 808150
Address	7th floor, Holborn Gate, 326-330 High Holborn, London WC1V 7PP

* Please select: Association, Industry, Ministry, Supervisor, EU Organisation, Other.

Disclosure of comments	
EIOPA will make all comments available on its website, except where respondents specifically request that their comments remain confidential. Please indicate if your comments should be treated as confidential, by deleting the word "Public" in the column to the right and leaving only the word "Confidential".	**Public**

Section 2 - Cyber risk for insurers		
#	**Question**	**Answer**
Q.1.	What is your view on the proposed relevance of loss factors as described in Table 1 and based on expert judgment? Please provide an explanation.	Agreed with regards impact type groupings.
Q.2.	What is your view on the main sources of cyber risk for insurers as described in sections 2.2 and 2.3? Are there any other relevant sources not covered in these sections? Please provide clarification.	Materially complete. The focus on malicious cyber attacks is fine as non-malicious is likely to be less material in impact and also less likely to be systemic unless it occurs at an essential Single Point of Failure (SPoF). Section 2.3.2, paragraph 63: Some incident Response Costs would be 1st party coverage (eg forensics and internal crisis management). Others would be 3rd party coverage eg credit report monitoring.
Section 3 – Key assumptions		
#	**Question**	**Answer**
Q.3.	What is your view on the proposed approach regarding operational errors (i.e. considering non-malicious events at a later stage)? Please provide clarification.	The most severe impacts are likely to result from malicious triggers rather than non-malicious. Therefore, capturing the malicious at this stage results in the capture of the greatest level of risk. The assumption makes sense given the difficulty in splitting out a frequency assumption for deliberate vs non-deliberate cause of outage at a service provider. Working assumption is that the materiality of this bias is low due to deliberate acts driving the frequency of material cyber incidents vs non-deliberate. However, it is important that the non-malicious triggers are incorporated at a later stage as consideration of this can be a forcing mechanism for

		insurers to better consider the operational risk resulting from internal human triggers and the appropriate controls to implement and monitor so that they can reduce this.
Q.4.	Par. 80 proposes a different treatment of the operational errors in case of in- and -outsource of operations. In the light of the potential biases introduced by the different in- out-sourcing operational models, please provide an indication on the materiality of such bias.	The key concern for the insurance industry is the uncertainty around the cost of a cyber catastrophe that impacts a large number of insureds. Reflecting the extent of outsourcing is important as the risk is entirely different to the risk from insourcing. The potential for lapses in IT can impact both those in-sourcing and out-sourcing but, whilst outsourced services should be more resilient, this is a source of aggregation and thus, if a significant outage occurs, this will give rise to a greater level of impact to both the insurer and many of its insureds. Further, non-malicious events can lead to large numbers of impacted insureds if this causes an outage for a cloud service provider. However, an outage caused with malicious trigger is more likely to lead to a large impact than one with a non-malicious trigger. Therefore, from a materiality perspective malicious intent is the most important to focus on.
Q.5.	What is your view on the proposed treatment of regulatory fines and compensation against legal actions? Please provide clarification.	Even if regulatory fines are excluded from the submitted scenario estimates, it is important that these are included as part of the overall narrative that accompanies a scenario. This will ensure that the participants carefully consider the materiality of the impact and whether the mitigation that exists is appropriate.
Section 4 – Scope		
#	**Question**	**Answer**
Q.6.	How do you assess the concentration of critical IT systems within group structures, i.e. are critical IT infrastructures such as the data center, the communications network (phone system, mail), management of critical	The extent to which critical IT systems are shared within an IT group is outside our area of expertise.

	applications, among others, often shared within an insurance group? Please provide clarification.	
Q.7.	Should stress testing of cyber resilience risk be carried out at group or solo level? Please provide clarification.	It is appropriate for group to have responsibility. As part of this, guidance could be included for the group to set clear guidelines for the entities to perform the assessment. Once the assessment is formed, a group function should collate the results and assess whether there is an adequate level of consistency within the group. In summary, performed at a solo level but on a consistent group basis with aggregation at the group level.
Q.8.	Should stress testing of cyber underwriting risk be carried out at group or solo level? Please provide clarification.	This would depend on the level of fungibility of capital between entities within a group. Capital is more likely to be fungible within a group that is all under one regulatory jurisdiction. However, we do not expect that this is the case for most groups under EIOPA supervision. As a result, the relevant regulator for each solo entity within the group will be interested in the results for the solo entities under its jurisdiction and it should be performed at this level.
Q.9.	What is your view on the considered hybrid approach to the scope definition, e.g. targeting groups for an assessment of cyber resilience risk and solos for an assessment of cyber underwriting risk? Please provide clarification.	Appropriate, for the reasons described in answers to Q's 7 and 8.
Q.10.	Which are in your view the Solvency II lines of business expected to be more impacted by affirmative cyber underwriting risk?	9. Other damage to property 13. General liability 16. Miscellaneous financial loss
Q.11.	Which are in your view the Solvency II lines of business expected to be more impacted by non-affirmative cyber underwriting risk (i.e. silent cyber risk)?	9. Other damage to property 10. Motor vehicle liability 11. Aircraft liability

		12. Liability for ships (sea, lake and river and canal vessels) 13. General liability 15. Suretyship 16. Miscellaneous financial loss 17. Legal expenses
Q.12.	What is your view on the criteria for the selection of the participating entities listed in Table 3? Please provide clarification.	Agreed.
Q.13.	Are there any other relevant criteria not covered in Table 3 or in your answers to the previous questions? Please specify.	There could be an additional consideration around the extent to which exclusions have been applied across the book. This could potentially be a filter at this stage, or could be left as an assumption that would bring any result of the non-affirmative stress test towards nil for a given organisation.
Section 5 – Scenarios		
#	**Question**	**Answer**
Q.14.	What is your view on the five selected scenarios for both cyber underwriting and cyber resilience risks? Please provide clarification.	Scenario 1 will test cyber resilience for all entities and cyber underwriting for just the small number of cyber writers for whom their cyber risk is sufficiently material relative to their total written premium. However, as exposure to cyber insurance risk grows across the market, it will test cyber resilience and underwriting risk across a greater spectrum of the market. With regards the subset exposed to Cyber Underwriting Risk,

		consideration of the application of natural perils exclusions (Eg earthquake or windstorm impacting data centre) should be taken into account. Scenario 2 is cyber resilience if it is a ransomware attack against the insurer itself and underwriting if on an insured. With regards Cyber Underwriting Risk it would be useful to consider whether this is truly systemic i.e. a single action leads to multiple insured impacted using a common threat vector vs. a campaign where similar action is taken repeatedly to impact multiple organisations. This will influence the scalability of the attack. Scenario 3 is cyber underwriting (and resilience if the insurer is impacted) but an extremely remote scenario given that the cloud service provider or infrastructure provider is likely to have failover plans in place and a high level of resilience. For this to occur and the outage to be of a significant length, the trigger would be more likely to have malicious intent. However, this would also have to be a sophisticated actor and the only financial gain could be from a benefit in any adverse impact on financial markets. Given that there would have to be a significant investment in instruments bought to benefit from this fall, this could be tracked and is therefore likely to attract law enforcement attention and prosecution. Scenario 3 is only useful to consider an extremely remote event and the resilience of the ecosystem to it. Scenario 4 is a very likely risk for both an insurer and insureds. It should be considered from a cyber resilience perspective. From a cyber underwriting perspective, it should be considered for some of the more material risks from a data breach but is likely to be a campaign rather than a true systemic shock. Comment in the 'Possible impact of the scenario on the insurance portfolio' around rep damage not being covered by usual policies. This is not necessarily true and should be considered on a case by case based on wordings. Scenario 5 is useful for both resilience and cyber underwriting. However, if the insurer is affected only a small set of the insureds is likely to be

		affected due to the diversity of power systems. Some key considerations that will influence results to this of scenario include (1) the application of infrastructure exclusions which tend to be applied on affirmative cyber policies and (2) work that has been done over the prior years to exclude cyber from other lines of business. Where there may be more exposure is personal lines / micro SME business where the buyer intends to have coverage from power outage regardless of cause of loss.
Q.15.	Which scenario do you consider most relevant from the list of scenarios proposed for cyber underwriting? Please provide clarification.	Scenario 2 "Ransomware / Data Theft" is the most likely event to occur and insurers should be encouraged to consider their exposure and actions that can be taken to reduce the policyholder risk e.g. cybersecurity practices
Q.16.	Which scenario do you consider most relevant from the list of scenarios proposed for cyber resilience? Please provide clarification.	Scenario 2 "Ransomware / Data Theft" is the most likely event to occur and thus the most important to test for resilience To the extent that an insurer has business critical reliance on a single service provider then the cloud outage / DoS scenarios may be a driver but this would be on a case by case scenario.
Q.17.	Are there any additional cyber risk stress scenarios that should be considered? If yes, please provide their narrative and specification.	Section 5.3 states that unauthorised transaction fraud has been removed. This risk may increase as the technology enables deception to become more convincing. This should be added in to test exposure to entities that may have significant losses.
Q.18.	What is your view on the separate treatment of the Ransomware and Data breach scenarios? Please provide clarification	Data breach could be dropped as extortion through disruption and data theft is prominent and covers the data breach risk.

Section 6 - Cyber Underwriting: Shocks, Specifications and Metrics		
#	**Question**	**Answer**
Q.19.	What is your view on the proposed metrics and indicators in terms of completeness and viability? Please provide clarification.	No comment
Q.20.	What is your view on the feasibility of splitting metrics for affirmative and non-affirmative coverages? Please provide clarification also with respect to add-on cyber coverages.	For non-affirmative, the portion being allocated to cyber perils varies significantly between insurers. This may require narrative to better differentiate the submissions. Another consideration would be to ask around the extent to which exclusions are applied. This will give a sense to which a book could be exposed to non-affirmative loss before the calculation is done.
Q.21.	What is your view on the feasibility of the metric "Expected losses if key exclusions are not applicable under stress"? Please provide clarification.	Different exclusions have a different confidence level. As a result, this can only be indicative. It may be appropriate to add a further stress test that is based on the exclusions most likely to break down but this is difficult to define.
Q.22.	What is your view on the approach to silent cyber approximation? Please add suggestions to improve it and provide clarification.	These are appropriate at this stage of maturity. However some elements are not clear: - For cloud outage and power outage what the length of duration and company type that leads to higher claims is. Higher is not defined. - The stock price decline from systemic ransomware could vary significantly. Not clear what this decline would be.
Q.23.	What is your view on the data collection? Is there any relevant information missing? Please provide clarification.	We think narrative discussing key assumptions made in the approach will be important.

		It may be useful to review the Oasis Loss Modelling Cyber Data Standards v1.0 which was released earlier in the year. It doesn't necessarily fit in here, but could be useful context with regards data collection standards.
Section 7 - Cyber Resilience: Shocks, Specifications and Metrics		
#	**Question**	**Answer**
Q.24.	What is your view on the assumed increase in operational and other costs due to a cyber risk event? Please provide clarification.	We agree with the method of allowing for these but a default option should be provided with participants encouraged to estimate the costs themselves and provide narrative to support any deviation.
Q.25.	What is your view on the proposed shocks in terms of completeness? Please provide clarification.	The proposed shocks are materially complete. However, the impact of the shock will need greater guidance to ensure consistency in estimation.
Q.26.	Do you agree that cyber resilience shocks are provided in technical terms, such as the duration of outage following a cyber event, or should they be prescribed also in terms of financial costs (i.e. monetary amount)? Please provide clarification.	Financial costs should not be prescribed but their calculation basis should be included within the submission.
Q.27.	What is your view on the proposed metrics in terms of completeness and viability? Please provide clarification.	Complete. However, some elements may need to be defined e.g. what is sensitive data for the data breach.
Q.28.	What is your view on the assessment of the impact of cyber resilience shocks at the level of business processes for all the scenarios? Would a more granular specification depending on the scenario (e.g. at IT systems level) be preferred? Please provide clarification.	At this stage this simpler process may be more appropriate for the submission. Companies should be encouraged to consider for their own internal purposes any more detailed impacts.
Q.29.	What is your view on the exclusion of ransom payments in the context of the ransomware scenario? Please provide clarification.	This may be appropriate given that the payment of ransoms should not be encouraged as it fuels further bad actor activity. In reality, this will be a function of the local legal environment and an individual organisation's internal standpoint. This may be an opportunity to ensure that Insurance risk boards have understood the local jurisdiction requirements for

		payments of ransom, have formed an internal view as to whether they would pay and have a response plan in place.
Q.30.	What is your view on the identified sources for the calibration of the shocks? Do you have any further suggestion on potential sources for the calibration? Please provide clarification.	Fine as a starting point. We cannot think of a comprehensive source so these will have to be considered and interpreted.
Q.31.	What is your view on the data collection? Is there any relevant information missing? Please provide clarification.	Useful to record all the qualitative information listed in addition to the quantitative.