|  |  |
| --- | --- |
| 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]](#footnote-2) and EIOPA’s rules on public access to documents[[2]](#footnote-3). 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 Please note that personal contact details (such as name of individuals, email addresses and phone numbers) will not be published.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]](#footnote-4) 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’. | |

|  |  |  |
| --- | --- | --- |
| Reference | |  |
| Name of the Stakeholder |  | |
| Type of Stakeholder (please delete in the column to the right the categories which do not apply) | Association, Industry, Ministry, Supervisor, EU Organisation, Other | |
| Contact Person |  | |
| Email address |  | |
| Phone number |  | |
| Address |  | |

\* 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 / Confidential** | |

|  |  |  |  |
| --- | --- | --- | --- |
| Section 2 - Cyber risk for insurers | | |  |
| **#** | **Question** | **Answer** | |
|  | 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. |  | |
|  | 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. |  | |
| Section 3 – Key assumptions | | |  |
| **#** | **Question** | **Answer** | |
|  | What is your view on the proposed approach regarding operational errors (i.e. considering non-malicious events at a later stage)? Please provide clarification. |  | |
|  | 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. |  | |
|  | What is your view on the proposed treatment of regulatory fines and compensation against legal actions? Please provide clarification. |  | |
| Section 4 - Scope | | |  |
| **#** | **Question** | **Answer** | |
|  | 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 applications, among others, often shared within an insurance group? Please provide clarification. |  | |
|  | Should stress testing of cyber resilience risk be carried out at group or solo level? Please provide clarification. |  | |
|  | Should stress testing of cyber underwriting risk be carried out at group or solo level? Please provide clarification. |  | |
|  | 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. |  | |
|  | Which are in your view the Solvency II lines of business expected to be more impacted by affirmative cyber underwriting risk? |  | |
|  | 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)? |  | |
|  | What is your view on the criteria for the selection of the participating entities listed in Table 3? Please provide clarification. |  | |
|  | Are there any other relevant criteria not covered in Table 3 or in your answers to the previous questions? Please specify. |  | |
| Section 5 - Scenarios | | |  |
| **#** | **Question** | **Answer** | |
|  | What is your view on the five selected scenarios for both cyber underwriting and cyber resilience risks? Please provide clarification. |  | |
|  | Which scenario do you consider most relevant from the list of scenarios proposed for cyber underwriting? Please provide clarification. |  | |
|  | Which scenario do you consider most relevant from the list of scenarios proposed for cyber resilience? Please provide clarification. |  | |
|  | Are there any additional cyber risk stress scenarios that should be considered? If yes, please provide their narrative and specification. |  | |
|  | What is your view on the separate treatment of the Ransomware and Data breach scenarios? Please provide clarification |  | |
| Section 6 - Cyber Underwriting: Shocks, Specifications and Metrics | | |  |
| **#** | **Question** | **Answer** | |
|  | What is your view on the proposed metrics and indicators in terms of completeness and viability? Please provide clarification. |  | |
|  | 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. |  | |
|  | What is your view on the feasibility of the metric “Expected losses if key exclusions are not applicable under stress”? Please provide clarification. |  | |
|  | What is your view on the approach to silent cyber approximation? Please add suggestions to improve it and provide clarification. |  | |
|  | What is your view on the data collection? Is there any relevant information missing? Please provide clarification. |  | |
| Section 7 - Cyber Resilience: Shocks, Specifications and Metrics | | |  |
| **#** | **Question** | **Answer** | |
|  | What is your view on the assumed increase in operational and other costs due to a cyber risk event? Please provide clarification. |  | |
|  | What is your view on the proposed shocks in terms of completeness? Please provide clarification. |  | |
|  | 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. |  | |
|  | What is your view on the proposed metrics in terms of completeness and viability? Please provide clarification. |  | |
|  | 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. |  | |
|  | What is your view on the exclusion of ransom payments in the context of the ransomware scenario? Please provide clarification. |  | |
|  | 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. |  | |
|  | What is your view on the data collection? Is there any relevant information missing? Please provide clarification. |  | |

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). [↑](#footnote-ref-2)
2. Public Access to Documents (See link: https://eiopa.europa.eu/Pages/SearchResults.aspx?k=filename:Public-Access - (EIOPA-MB-11-051).pdf). [↑](#footnote-ref-3)
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). [↑](#footnote-ref-4)