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Please note that personal contact details (such as name of individuals, email addresses and phone numbers) will not be published.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	Institut des actuaires - France
Type of Stakeholder (please delete in the column to the right the categories which do not apply)	Association
Contact Person	Samuel Cywie
Email address	Samuel.cywie@institutdesactuaires.fr
Phone number	+33(0)650273124
Address	4 rue Chauveau-Lagarde, 75008 Paris, France

* 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.	The proposed approach does not take into account the combination of attacks and types of attacks or their intensity. The "low, high" gradation is subjective and will depend on the point of view of different insurers.
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.	Paragraph 76 gives the impression that the scenarios considered are exhaustive, whereas an incentive towards the emergence of more "personalized" scenarios (making it possible to take into account possible fragilities linked to the seasonality of a market or an activity) should be recommended as well as stochastic scenarios, as in finance.
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.	This separation can be limiting when working on operational impacts and associated resilience means: putting in place effective means of restart and resilience must deal with blockages or major data losses, whether they are the result of "malicious" or unintentional actions; often, blockages or losses will have the same type of operational impact, regardless of the origin of the disaster We should also try to make an inventory of the "systemic" tools, i.e. shared by the sector, and to question their possible degree of business continuity.
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	We agree with the proposal to treat interruptions (deliberate or not) in the same way with the subcontractor, who must ensure a global quality of service, to be evaluated and supervised by the delegator.

	introduced by the different in- out-sourcing operational models, please provide an indication on the materiality of such bias.	Nevertheless, it is difficult to audit external tools, and it is necessary to encourage a sufficiently high level of requirement for these tools. It would be counterproductive to push companies to develop internal solutions of poor quality, which could then be audited more easily but which would be of mediocre quality.
Q.5.	What is your view on the proposed treatment of regulatory fines and compensation against legal actions? Please provide clarification.	We should encourage local exercises.
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 applications, among others, often shared within an insurance group? Please provide clarification.	Impact assessment, detection and resilience means must integrate the interaction with the Group's systems, either from a negative perspective (too much interconnection) or from a positive perspective (mutualization of resources and detection and resolution methods). However, the situation differs from one organization to another, and some Group subsidiaries may be more exposed to a concentration of large subcontractors (cloud, data-center, networks) than to the systems of the Group they belong to.
Q.7.	Should stress testing of cyber resilience risk be carried out at group or solo level? Please provide clarification.	Although each entity must be responsible, it is preferable to share with the Group in terms of scenario definition, management crisis management and rapid consolidation of impacts, especially if the systems are highly interconnected.
Q.8.	Should stress testing of cyber underwriting risk be carried out at group or solo level? Please provide clarification.	Each entity should carry out its own stress tests, as the types of contracts may be specific (although the impacts and results are consolidated at Group level), especially if the Group is not homogeneous in terms of business lines (e.g., insurance subsidiary in a banking group).
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	Local and business-specific solo visions are essential.

	and solos for an assessment of cyber underwriting risk? Please provide clarification.	An aggregation of the results at group level is necessary, taking into account the propagation and extension effects between entities.
Q.10.	Which are in your view the Solvency II lines of business expected to be more impacted by affirmative cyber underwriting risk?	Civil Liability & business interruption.
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)?	Civil Liability & business interruption.
Q.12.	What is your view on the criteria for the selection of the participating entities listed in Table 3? Please provide clarification.	It is urgent that an ecosystem of economic and financial protection of all financial and industrial activity be put in place. This will only be possible if an actuarial database is set up and shared between all stakeholders. The European authorities must force all economic actors to share cyber claims data in complete confidentiality (anonymization methods exist to guarantee confidentiality).
Q.13.	Are there any other relevant criteria not covered in Table 3 or in your answers to the previous questions? Please specify.	It is urgent that an ecosystem of economic and financial protection of all financial and industrial activity be put in place. This will only be possible if an actuarial database is set up and shared between all stakeholders. The European authorities must force all economic actors to share cyber claims data in complete confidentiality (anonymization methods exist to guarantee confidentiality).
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.	Given the malicious nature of cyber risk, special attention must be paid to cyber risk communication to avoid making risks self-fulfilling. Common scenarios are necessary but not sufficient. Specific scenarios for each entity can be considered. The scenarios will have to be reviewed on a regular basis given the evolving nature of cyber risk.
Q.15.	Which scenario do you consider most relevant from the list of scenarios proposed for cyber underwriting? Please provide clarification.	
Q.16.	Which scenario do you consider most relevant from the list of scenarios proposed for cyber resilience? Please provide clarification.	
Q.17.	Are there any additional cyber risk stress scenarios that should be considered? If yes, please provide their narrative and specification.	
Q.18.	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**
Q.19.	What is your view on the proposed metrics and indicators in terms of completeness and viability? Please provide clarification.	Of particular importance is the return period ie the length of time after which business is restored. Metrics will need to be revised regularly as the cyber risk rapidly changes.
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.	Non affirmative coverages cannot be part of the stress tests.

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.	It is feasible and necessary (e.g. Definition of Cyberwar).
Q.22.	What is your view on the approach to silent cyber approximation? Please add suggestions to improve it and provide clarification.	Silent cyber cannot be correctly evaluated therefore we do not support the approach to silent cyber approximation.
Q.23.	What is your view on the data collection? Is there any relevant information missing? Please provide clarification.	It is urgent that an ecosystem of economic and financial protection of all financial and industrial activity be put in place. This will only be possible if an actuarial database is set up and shared between all stakeholders. The European authorities must compel all economic actors to share cyber claims data in complete confidentiality (anonymization methods exist to guarantee confidentiality). The claims database should not be too aggregated to be usable.
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.	Faced with the increase in cyber risk, it is essential to fight and strengthen security within companies. But for these actions to be effective and properly prioritized, it is equally essential that their effect on the economic impact of attacks be measured. Measures must be taken based on impact studies.
Q.25.	What is your view on the proposed shocks in terms of completeness? Please provide clarification.	The proposed shocks seem to us to be relatively complete, even if it seems difficult to anticipate all the possible shocks that could occur.
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	Yes, but there are specificities to be taken into account from one player to another (for example: different exposure to denials of service depending on the sector of activity, seasonal vulnerability of the activity,

	prescribed also in terms of financial costs (i.e. monetary amount)? Please provide clarification.	etc.), especially in cyber underwriting. This variability is not considered in the shocks, which are essentially frequency shocks. In addition, the duration of the unavailability of the means of production seems interesting to specify as such; it is often difficult to transcribe in financial equivalent (loss, loss of profit).
Q.27.	What is your view on the proposed metrics in terms of completeness and viability? Please provide clarification.	The return to business as usual can be very long, it can take months, years, or even never happen. It is necessary to break down into different levels of business recovery.
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.	The scenarios should be defined at group level and the impact study done at the level of each entity and business line.
Q.29.	What is your view on the exclusion of ransom payments in the context of the ransomware scenario? Please provide clarification.	The question of whether or not to pay the ransom is not much of a shock in a scenario. Especially since paying the ransom never totally solves the problem (cf Colonial Pipeline which did not recover all of its data, plus the need to plug security breaches and identify them so that it does not happen again). Considering the ransom payment as a parameter would also be a bad signal, reinforcing the appetite of hackers to get information about ransom guarantees from insurers.
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.	The sources have important reliability problems, for instance: lack of transparency about their constitution, bias (they rely on victim statements) and a lack of impact measurement. These sources have not been constituted for the calibration of shocks.
Q.31.	What is your view on the data collection? Is there any relevant information missing? Please provide clarification.	Data collection is lacking at the global level but also within companies. An obligation for all economic actors to share cyber loss data in complete confidentiality would also help companies to organize their internal data collection.

		It will be necessary to support companies in the organization of data collection, which can be complex. As the DORA regulation is likely to create standards for the definition of claims, a convergence would be desirable.