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Please note that personal contact details (such as name of individuals, email addresses and phone numbers) will not be published.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	Actuarial Association of Europe
Type of Stakeholder (please delete in the column to the right the categories which do not apply)	Association
Contact Person	Monique Schuilenburg
Email address	moniques@actuary.eu
Phone number	003222016021
Address	1 Place du Samedi, B-1000 Brussels, Belgium

* 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.	Before we elaborate on question Q.1, we would like to make a basic comment on the draft of the stress testing component for cyber: It is essential that the stress testing component for cyber, in addition to the selection of relevant cyber scenarios suggested here in Table 1, includes a general definition and classification of cyber risks (e.g. a well-defined risk taxonomy) that provides an exhaustive and consistent way to differentiate the effects due to cyber risks, also from other risks. Possible ideas for the design of such a taxonomy can be found in the result report of the DAV AG Cyber "Daten und Methoden zur Bewertung von Cyberrisiken" (https://www.researchgate.net/publication/346897134_Daten_und_Methoden_zur_Bewertung_von_Cyberrisiken_-_Ergebnisbericht_des_Ausschusses_Schadenversicherung_AG_Daten_und_Methoden_zur_Bewertung_von_Cyberrisiken) , the VERIS-Standard (Vocabulary for Event Recording and Incident Sharing) (http://veriscommunity.net/) or the proposed taxonomy in the CRO-Forum (https://www.thecroforum.org/wp-content/uploads/2018/02/201802_CROF_Capture_and_sharing_of_digital_event_data.pdf). This is necessary to achieve a uniform interpretation of the selected scenarios in the current consultation and to enable a targeted extension of the stress test framework for the cyber component in the future. Please also refer to our answer of question Q.2 for further ideas on a potential definition and classification of cyber risks. In addition, the distinction between cyber risks and operationals risk is unclear in some places (e.g. question Q.3). Also from this point of view, we would very much appreciate a general definition and classification of cyber risks, that allows a clear distinction between cyber risks and operational risks. A lack of clarity might lead to the double counting of risk. In the following comments, we focus on the five scenarios that should remain in the stress test framework (Ransomware, DoS, Data breach and Data Centre/Infrastructure damage (cloud outage), Power outage) and do not comment on the three scenarios that are not considered (Cryptojacking, Unauthorised transaction and Payment infrastructure outage). In principle, we do not have any objections to the selection of the relevant scenarios Ransomware, DoS, Data breach and Data Centre/Infrastructure damage (cloud outage), but we would like to point out the need for a clear taxonomy for

		cyber risk, as mentioned above. In addition, we would like to share the following thoughts on the individual scenarios selected: - In case of the Power outage scenario we see cyber as only one of many conceivable triggering events and, due to the relevance of power outage risk, advocate integrating the scenario into a higher-level stress testing framework, e.g. the operational risk stress testing. - In our opinion, the DoS scenario is outdated. A service provider failure /outage instead of infrastructure/cloud might be a more appropriate alternative. - The scenarios Data Center / Infrastructure (Cloud outage) and Power outage seem to be somewhat related and could be considered as one scenario with different risk factors. - The Data breach and Ransomware scenarios seem to be somewhat related as well and could be considered as one scenario with different risk factors. Phishing attacks should also be seen as a relevant cyber scenario. Such attacks have also led to serious cyber events according to the study "Cyberangriffe gegen Unternehmen in Deutschland" by Dreißigacker, von Skarczinski and Wollinger (see page 127). The assignment of the categories "High", "Moderate" and "Low" to describe the impact of a cyber scenario on an insurance undertaking according to Table 1 is not a priori transparent and it is not clear on which basis the categorisation has been performed. Furthermore, we come to a different assessment in the following cases: 1. Scenario Ransomware: Assignment of the category "Moderate" for the expected direct loss is not plausible in our opinion. We would expect the category "High" to be assigned here. We essentially attribute this to the findings in the above-mentioned report of "Cyberangriffe gegen Unternehmen in Deutschland " according to which ransomware is listed among the top 3 most serious attacks. 2. Scenario Data breach: We tend to see a higher risk than in the "Moderate" category for potential loss of reputation and would regard the "High" category as adequate. 3. Scenario DoS: In our opinion, assigning the category "Low" for the expected loss of reputation might be rather too optimistic, if one considers that e-mail and communication systems as well as the advertising presence of companies are typically affected as a result of a DoS attack. Both systems are essential for interaction with customers and consequently we would prefer the "moderate" category here.

		While we acknowledge that it is difficult to generalise the impact of cyber risks, loss arising from reputational damage is country- and entity-specific, and may vary over time (e.g. following previous cyber risk event). This loss factor could be determined by the entity itself as part of its stress and scenario testing.
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.	In our view, sections 2.2 and 2.3 take into account all relevant sources of cyber risk for the insurance industry. In addition to the description in 2.2 and 2.3, we propose to differentiate *targeted (idiosyncratic) attacks* and *non-targeted (systemic) attacks* as well as *accident and failures* as separate root causes analogous to "A comprehensive model for cyber risk based on marked point processes and is application to insurance" by G. Zeller and M. Scherer. Furthermore, we think that non-targeted attacks should be considered in the stress testing framework due to their relevance. Non-targeted attacks have the potential to have an impact on larger parts of the portfolio, while targeted attacks are causing claims for just a few contracts. However, many of the primary cyber standalone policies are offering limited coverages, therefore large single claims (for targeted attacks) are becoming for many insurers less relevant compared to non-targeted attacks. We think that the differentiation into different root causes (targeted attack, untargeted attacks and accidents/failure) results in a higher degree of clarity and comprehensibility of the scenarios.
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.	We would highly appreciate, if non-malicious events can be considered right at the beginning of the cyber stress testing framework. In our opinion this makes sense because the impacts of non-malicious events differ from those of malicious events: For example, in the case of data breaches, non-malicious events tend to have lower damage levels than malicious attacks. Irrespective of the question of whether non-malicious events are considered from the beginning or at a later stage during the development of the stress testing framework, we would like to strengthen the need for a comprehensive and uniform definition and classification of cyber risk (see also comments on question Q.1 and question Q.2).

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.	It is difficult to quantify the materiality of this bias when a consistent definition and classification is still missing (see also comments on questions Q.1 and Q.2). We agree that there is a risk of penalising those with outsourced systems relative to those with full in-house capabilities, but the extent of this would vary on a case by case basis and is difficult to generalise. One could argue that those with in-house models are likely to have a larger concentration risk arising from an operational error, in which case the impact would be more severe than a model with a diverse set of outsourced providers. The described risk should already be covered in the existing operational risk processes. Nevertheless it seems crucial that insurers capture disruptions caused by an interruption of services by a service provider in a comprehensive way. But this goal should be achieved without creating a bias.
Q.5	What is your view on the proposed treatment of regulatory fines and compensation against legal actions? Please provide clarification.	Given the potential significance of these types of regulatory fines, it would seem remiss not to include this as part of a cyber risk stress test. We note that historical data has been provided in other sections of the paper. A database of regulatory fines or awards of compensation (where public) would be useful for entities to adequately assess the impact of a cyber risk event. Despite the additional complexity involved, taking these cost components into account is needed for a realistic approach. A compromise would be to consider regulatory fines and compensations against legal actions at a later point in time in the cyber stress test framework.
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	Insurance groups are very heterogeneous in terms of the level of concentration of their critical IT systems. Nevertheless, even if IT systems are not fully centralized, these systems are generally strongly interconnected and often rely on common underlying infrastructures. There are often local hubs (i.e. centralization on a lower than group level) and the systems are subject to common standards, standardized IT management approaches and governance. Please refer to question Q.7 for further considerations.

	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.	Cyber resilience stress testing at a group level would seem more appropriate given the potential high-level of interdependencies between entities (both insurance and non-insurance) within a group. This overall assessment will not only help from a supervisory point of view but will potentially also create a good benchmark for insurance groups in favour of their overall cyber resilience. However, we do note that local supervisors or a Board of Directors may be keen to see this at a solo level as some material risks to a solo entity may be missed if they are less material at group level.
Q.8	Should stress testing of cyber underwriting risk be carried out at group or solo level? Please provide clarification.	Due to potential concentration of cyber underwriting risks within a group, a solo cyber underwriting stress seems more appropriate and could provide more insightful results. This seems like it might give more sensible results; the group results may be more difficult to break down in terms of diversification, aggregation, etc. However, an area of interest may be the extent to which there is intra-group reinsurance. These interdependencies may be missed when investigated from a solo perspective only. But it should be ensured that there is a reliable accumulation control on group level, and potential accumulation effects from underwriting stresses across a group should be taken into account. We would also like to point out that certain stresses can have effects on both sides of the balance sheet. If necessary, group level effects could be explicitly included at a later stage, also to assess the diversification effects within the 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 and solos for an assessment of cyber	In general, we agree that the hybrid approach might be the most purposeful way. Operational risks and underwriting risks are handled separately within entities and therefore the analyses are not related to each other. Therefore even if the stress testing is targeting the same level, the results will be independent from each other. If a stress scenario affects both the resilience of the insurance group and of the local underwriting, and there is a need for an overall risk assessment, it will of course be necessary to establish a proper aggregation methodology in order not to underestimate the combined effects.

	underwriting risk? Please provide clarification.	
Q.1	Which are in your view the Solvency II lines of business expected to be more impacted by affirmative cyber underwriting risk?	Depending on the scenario, different lines of business might be affected, e.g. a power outage scenario might affect a wide range of lines of business. In general the LoB "General liability insurance" might be more impacted by affirmative coverages due to cyber standalone policies, but also by General Liability in general and Financial Lines policies. But also lines of business where cyber-related modules are covered through extensions are impacted like the LoBs 7 – fire and other damage to property insurance 8 – general liability insurance 12 – miscellaneous financial loss
Q.1	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)?	The insurance industry has taken decisive steps in the management of non-affirmative cyber coverages, however, there still might be business where non-affirmative cyber coverage exists or at least the risk is not adequately addressed by the relevant processes (e.g. pricing, risk management). The lines which might still be impacted by these circumstances are 6 - Marine, aviation and transport insurance (potentially - all transport vehicles use technology to some extent for navigation etc, so this naturally creates the possibility for losses for these products. Of course, there is scope for dispute over where the coverage sits or whether there is recourse from another party in these cases (e.g. if self-drive cars are hacked, does this fall under the motor liability policy or manufacturer's product liability or warranty?) 9 – credit and surety insurance 10 – legal expense insurance 12 – Miscellaneous financial loss But also LoBs where secondary effects of cyber related events are covered might be impacted, e.g. business stemming from contingent business interruption and legal expense.
Q.1	What is your view on the criteria for the selection of the participating entities listed in	In general, high-level market share metrics for cyber resilience & non-affirmative exposures make sense. For affirmative exposures, this should be as specific as possible. It may be worth considering the inclusion of an over-arching

	Table 3? Please provide clarification.	proportionality metric similar to those introduced in the latest ITS on reporting & disclosure so as not to impose overly onerous requirements on small undertakings in the first instance. Cyber resilience: If cyber resilience is measured at the group level (see comments on Q.7), the criteria reference benchmark, exposure and metrics given here are appropriate in our opinion. Cyber underwriting: For the cyber underwriting scenarios, we also consider the criteria given in Table 3 to be appropriate.
Q.1	Are there any other relevant criteria not covered in Table 3 or in your answers to the previous questions? Please specify.	**Cyber resilience:** In addition to the criteria proposed in Table 3, we would consider it beneficial to include further companies that represent systemically important companies for a country or for the EU, e.g., in the sense of the IAIS assessment. An additional criterion for the selection of systemically important institutions can be obtained from the current overview of European financial conglomerates, i.e. companies that are active in both the banking or investment services industry and in the insurance industry. The size of the company plays a subordinate role for the categorization as financial conglomerate; more relevant can be, e.g., the fact that a company of a group is active in the insurance industry or that a company from the insurance or banking industry is active to a considerable extent in the respective other industry (for an overview of the relevant criteria, see the Financial Conglomerates Supervision Act FKAG). **Cyber underwriting:** In addition to the criteria proposed in Table 3, we think it would be useful to use risk-adjusted parameters from internal management, e.g. the return period of a scenario in relation to the associated premiums. In addition to the gross values (GWP, gross TP), which are used in the metrics, the net values should be considered for the selection of the companies. In the case of exposure values, net exposures should also be chosen rather than gross exposures. Sum insured & policy information from the new S.14.03 Cyber Underwriting QRT (once this is implemented) could be used for affirmative risks.

Section 5 - Scenarios

#	Question	Answer
Q.1	What is your view on the five selected scenarios for both	We don't have a strong view on additional scenarios to include, or scenarios to exclude from the five provided. Some seem to be more relevant for underwriting and some more relevant for resilience, though.

	cyber underwriting and cyber resilience risks? Please provide clarification.	The scenarios on Data Center /Infrastructure Damage (Cloud Outage) and Power Outage seem to be somewhat related and could be considered as one scenario with different risk factors. The same might be true for some of the other scenarios, like for the data breach and ransomware scenario. These two seem also pretty linked to each other. Moreover, the ransomware scenario seems to be less of a scenario, but more a consequent loss event.
Q.1	Which scenario do you consider most relevant from the list of scenarios proposed for cyber underwriting? Please provide clarification.	Relevance depends significantly on entity specific circumstances. The Data Breach scenario seems at first glance the most relevant for cyber underwriting, as it can affect both the daily operating business of the insurer itself, but it can also directly impact new business, as it has a potential risk of not adequately underwritten business. Also client data being breached is very relevant for cyber criminals, as client data is very valuable for companies. In addition, ransomware scenarios could be quite severe given the large losses in the tail of the loss distribution. As side note, from a silent cyber perspective, one could consider a business continuation contract that would be affected from, e.g., a power outage or ransomware attack, preventing the insured company from doing business for a period of time.
Q.1	Which scenario do you consider most relevant from the list of scenarios proposed for cyber resilience? Please provide clarification.	Relevance depends significantly on entity specific circumstances. Given the very large volumes of especially classified, personal or even health specific data used by (re)insurance companies, assessing a data breach scenario could be particularly informative. The Data Center /Infrastructure Damage (Cloud Outage) scenario seems to be most relevant for cyber resilience. The detailed listing suggests that the daily operations are affected the most by the mentioned risk factors.
Q.1	Are there any additional cyber risk stress scenarios that should be considered? If yes, please provide their narrative and specification.	A possible suggestion for an additional scenario is a very intense cyber incident where you lose all access to your system forever and have to 1) recover data, and/or 2) develop a new system from scratch. Another suggestion is a cyber incident, in which data is altered in such a way that payments are manipulated (Tesco Bank case study).
Q.1	What is your view on the separate treatment of the Ransomware and Data breach	The current split of these scenarios seems reasonable, as the underlying source and possibly the coverage by a cyber insurance differs, and therefore can be treated as a different risk. However, this answer should also be read in conjunction with different definitions and a better specification of a scenario and a loss type.

	scenarios? Please provide clarification	
Section 6 - Cyber Underwriting: Shocks, Specifications and Metrics		
#	**Question**	**Answer**
Q.1	What is your view on the proposed metrics and indicators in terms of completeness and viability? Please provide clarification.	In general, we have no objections regarding the proposed metrics and indicators. However, from a risk perspective the utilization of limits is also relevant when addressing the question if the risk is within the risk appetite of the undertaking. While it may be difficult to standardise, a qualitative metric on the liquidity impact of the scenario could add value to the exercise.
Q.2	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.	In general, we agree that the metrics for affirmative and non-affirmative coverages should differ. For some lines of business, this seems to be possible, however, it may be very challenging for others depending on the scenario. But in the end each product needs to be assessed individually. The approach might be relatively similar for affirmative and non-affirmative cyber coverage as for both multiplicative or frequency-severity approaches with the application of factors determining the probability of affection and severe of claim might be used. While metrics for affirmative covers can certainly be based on detailed information, it might be a stretch to expect the same for non-affirmative cyber coverage. Especially as the peril is constantly subject to change and hence changes in affected lines of business and types of coverage are to be expected.
Q.2	What is your view on the feasibility of the metric "Expected losses if key exclusions are not applicable under stress"? Please provide clarification.	This seems to be a viable metric given current developments in consumer protection and legislation which can impact losses as, example.g., in the COVID-19 pandemic and business interruption insurance: we have observed that it's possible that governmental pressure may results in a policyholder-friendly outcome when interpreting policy wordings in some coutries. Wherever uncertainties exist, we agree that expected losses should be considered as if exclusions are not applicable. Nevertheless, the variety of existing exclusions, even of the most widely used ones, is large. The schematics of the exclusions differ so much that from our point of view a simultaneous failure of all of them is a rather unrealistic basis for a shock.

		In addition, expected losses should be considered if reinsurance is not responding as expected. This is especially important to non-affirmative covers as reinsurance exclusions are often stricter than insurance exclusions and therefore do not offer back-to-back coverage.
Q.2	What is your view on the approach to silent cyber approximation? Please add suggestions to improve it and provide clarification.	The example for Professional Indemnity (PI), Errors & Omissions (E&O) and Director's & Officer's (D&O) has its relevance for the insurance business and is very helpful to understand the approach for silent cyber coverages. However, clarification on assessing the probability of the negative outcome of a court case might also be helpful as several factors driving the assessment (factors that the insured facing the attack, suffering losses from the attack, losses driven by breach of duty and demonstrability of the breach of duty). The probability of a negative outcome of a court case might be in the end low, but not negligible. The application of the proposed exemplary shocks might lead to only roughly estimated results for reinsurance undertakings as a lot of the necessary information is not available (e.g. whether ransom payments are insured in which policies and with what sub-limits).
Q.2	What is your view on the data collection? Is there any relevant information missing? Please provide clarification.	We agree with the scope of the data collection. However, it is becoming more and more usual to insert sub-limits and exclude certain parts of typical coverages. These would need to be applied on a more granular level. On the other hand, the data collection is more detailed than commonly available on reinsurance level, especially w.r.t. the proposed template in the annex.
Section 7 - Cyber Resilience: Shocks, Specifications and Metrics		
#	**Question**	**Answer**
Q.2	What is your view on the assumed increase in operational and other costs due to a cyber risk event? Please provide clarification.	It may be more straightforward to model an increase in costs primarily via an increase in payouts as they fall due, with provisions established for large, one-off costs post-event, as provisioning for all cost increases at time 0 would provide an immediate shock to the balance sheet which may be unrepresentative of how the scenario would emerge in reality. Depending on the nature of the scenario, it may also be necessary to reflect a change to the expense assumption used to model the technical provisions.

		A cyber event would most probably trigger costs for external support (e. g. external experts to assess potential damage) and also costs for recovering the status quo before the attack / event.
Q.2	What is your view on the proposed shocks in terms of completeness? Please provide clarification.	In general the proposed shocks seem to cover most of the possible main events in the context of cyber risks and seem to be an adequate fit for a scenario set. For the fifth scenario (power outage) one could argue that this scenario might only partly be caused by a cyber event or it might in some cases be difficult to determine, if a cyber event caused the power outage or if it was caused by another operational risk.
Q.2	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.	As the impact on insurers can be quite different depending on their business model and individual operational processes it seems adequate to provide just shocks in technical terms. The technical terms are also more easily linked to different exposures in the business. Providing a quantification of financial costs could help simplify the scenario testing process. However, we acknowledge that some financial costs are dependent on the specific circumstances of the entity. Specifying the financial costs for different aspects of the scenario would still be helpful as a benchmark.
Q.2	What is your view on the proposed metrics in terms of completeness and viability? Please provide clarification.	The proposed metrics seem adequate in general. Nevertheless we would suggest a reduced number of metrics as more metrics covering the same effect could make interpretations more complex. The first three metrics (Time elapsed until return to business as usual, Business processes affected, Operational and other costs) seem to be enough to cover the resulting effect from an event and make it sufficiently transparent. One could suggest to (additionally) determine the effect on the solvency ratio if – and only then – the adverse effect is material in the context of the insurers solvency ratio. Otherwise there is no real added value from this additional metrics. Moreover one could consider adding potential secondary losses (liability cases) that could emerge when 3rd parties or partners are affected, but the potential magnitude of this is not described. While it may be difficult to standardise, a qualitative metric on the liquidity impact of the scenario could add value to the exercise.

Q.2	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.	For some scenarios (see also answer to question Q.25) a more helpful approach would be to determine the impact on the undertaking. Especially the scenarios Ransomware and Data Breach might have often the same trigger event (as also described in the paper) and it therefore seems to be necessary to specify the scenarios more granularly and make clear how they differ.
Q.2	What is your view on the exclusion of ransom payments in the context of the ransomware scenario? Please provide clarification.	This does not seem unreasonable at this time for cyber resilience scenarios given the different focus compared to cyber underwriting. There exist reasons not to include ransomware payments (e. g. supply in the market for relevant covers with the increase of ransomware attacks). Nevertheless, it would be helpful to eventually consider all options for the insurer and to include the specifics of its cyber insurance policy in the scenario (i. e. cover for ransomware payments). Otherwise not all risk mitigation techniques currently available in the market are adequately considered.
Q.3	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.	Tesco Bank case study, see answer to Q. 17
Q.3	What is your view on the data collection? Is there any relevant information missing? Please provide clarification.	Tesco Bank case study, see answer to Q. 17