Cyber risk for insurers	Type	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.	Response
Insurance Europe	Association	The industry would like to note that any stress test exercise should have clear objectives, appropriate timescales and be proportionate to its objectives. Specific comments on the proposed relevance of loss factors are as follows: •In terms of ransomware, direct losses are low when systems are restored quickly enough. However, there tends to be competing factors in practice, such as the extent of encryption and the quality of backups. Therefore, the rating of moderate is plausible. •The denial of service is a relevant scenario but, in general, not deemed significant. For most insurers and pension providers, an outage would need to be of a long duration to be significant. “Simple” denial-of-service attacks can usually be mitigated rather quickly. In addition, denial of service rarely affects all services (which are usually not in the same place because of the multiplication of SaaS services) and is, in most cases, for a relatively short time. Insurance companies seem less affected by these services. •For data breach, the impact on “Restoration” should not be “moderate”: it should be “low”, unless the scenario is for both “data theft and deletion of the copy held by the undertaking”. The restoration indeed does not impact the recovery (a company will tend to correct the flaw in question rather than restoring to a version that is likely to have the same flaw or is obsolete). •There is no link between availability and cryptojacking. •For the payment infrastructure outage, it would be low, except if the unavailability affects systems supporting tax declarations and if the amounts are evaluated as “moderate”. •The "Data Center / Infrastructure" scenarios are usually not the consequence of a cyber act but rather the consequence of an event (for example, natural disaster) affecting IT infrastructures. It is rather a scenario associated with a technical stress. In the cases where a “Data Center/ Infrastructure” scenario occurs as a result of a cyber-attack, this may be significant if infrastructures are shared across a group and there is an additional cost for policyholders to check data and systems to ensure that they have not been corrupted. Therefore, if the “Data Center/ Infrastructure” scenario should be implemented at all, the nature of the drivers should be taken into account in the design of this scenario. •As for power outage, it should be low for direct losses to be consistent with other scenarios. However, a point can be made that out of all scenarios proposed, power outage may be argued to not be included since it is primarily caused by external factors and is not dependent on the maturity of a company in their ability to deal with cyber risk. Therefore, the relevance of having this scenario within a cyber stress test is questioned. •“Unauthorized transaction” is a plausible scenario which could trigger important losses. This scenario should be retained.	Clarifications addressing some of the comments regarding rationale for the low/moderate/high rating system and scenario selection in Table 1 were added to the text. Moreover, after consideration a number of the proposed changes to the specific impacts were also taken on board. More specific comments regarding the scenarios are dealt with in chapter 5, which describes them in detail.
GDV	Association	Seems plausible.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry	We have a number of observations: For the scenario “Data Breach”, the impact on “Restoration” should not be “moderate”: it should be “low” unless the scenario is for both “data theft and deletion of the copy held by the undertaking”. For the scenario “Power outage”, the impact on “direct loss” should be “low” (and not “moderate”) for the same reason that direct loss impact on data center is low. For the “DoS” scenario, the “availability” impact depends on what systems are targeted by the “DoS” attack (e.g., production or monetary): in a worst-case scenario, the impact might be “high” if the IT systems of the insurance company are not available; in other cases (e.g., customer website), actual impact should be considered as “moderate”. Ransomware could have a higher impact on direct loss (potentially very high) and on reputation, likely the same level as a data breach. Depending on cloud usage a data center/cloud outage could have higher direct loss. What is not considered is supply-chain attacks which are often a vector nowadays. We note EIOPA mentions reputational risk, where we note the challenges of quantifying this. In addition, EIOPA should clarify how the business interruption loss should be quantified (e.g., which loss components should or should not be taken into account).	

METAMETRIS	Consulting	In our opinion, the structure of loss described in table 1 doesn't fully reflect the nature of the risk. "Direct loss" covers potentially all impacts except Loss of reputation and could split into: -Cost of recovery including cost of additional working hours to compensate backlog as well as system restoration costs (which may be the first impact for an insurance company), -Loss of revenues covering loss of new business as well as increased client attrition, -Legal and regulatory impact, -Other financial losses (including ransom), Legal and regulatory impact may be extremely significant with GDPR and even more with DORA and should be included in the stress test assessment.	
Cowbell Cyber	Industry	Agreed.	
IfoA	Association	Agreed with regards impact type groupings.	
Cyber risk for insurers	**Type**	**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.**	**Response**
Insurance Europe	Association	The main sources of cyber risk for insurers identified are sufficient for the most part, but a few points may be addressed: •It could have been beneficial to discuss the use of legal protection following a disclosure of information incident (in reference to paragraph 2.3 and the exploration of extreme motor insurance scenarios). •For the types of cyberattacks listed in section 2.2.3, there is no reference to vulnerabilities exploitation vendor software/hardware compromise as relevant. •There is no explicit reference to existing controls and their role in risk reduction, such as multifactor authentication or remote access management.	Overall, the comments on the presented thoughts on drivers of cyber risk were positive. As further improvement, multiple details in the paper have been updated to reflect stakeholders' comments, especially regarding attack vectors and state-linked criminal actors. Note that some of the comments, especially regarding non-malicious incidents and specific scenarios are taken into account in other sections of the paper.
GDV	Association	Regarding cyber underwriting risk we overall agree with the described sources of cyber risk.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry	Impact on people (personnel or clients) when speaking about critical systems (e.g., railroads, IoT's, OT in production, vehicles, etc.) is missing or not explicit enough. This might have an impact in other insurance products. Parts of this assumption are already in the silent cyber part (fire/property or workers compensation) Supply-chain (3ed party) risk should be considered.	
METAMETRIS	Consulting	The main source of cyber resilience risks for insurers are clearly criminal organizations. For cyber underwriting risks additional sources of risk depending on the targeted company can be considered such as nation states for Operators of Essential Services or competitors for companies exposed to industrial espionage.	
Cowbell Cyber	Industry	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 SPoF.	
IfoA	Association	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.	
Key assumptions	**Type**	**What is your view on the proposed approach regarding operational errors (i.e. considering non-malicious events at a later stage)? Please provide clarification.**	**Response**
Insurance Europe	Association	Overall, the approach is sufficient. However, the potential impact/likelihood ratio seems low. From the perspective of immediate mitigating measures, the treatment of malicious and non-malicious events in the context of a stress test is comparable. There are significant differences in the further (post-) treatment (for example, in the context of offender investigation and prosecution). However, there are some instances where malicious and non-malicious events must be treated separately, as the nature of the risk may be different for malicious events.	The inclusion of non-malicious events in the framework since the beginning received split comments. Content-wise the stakeholders' views converge on the following facts: - independently of the malicious or non-malicious nature of the event, the immediate impact on the operations is comparable; - malicious acts are (usually) characterised by low frequency and large impact; - non-malicious acts are (usually) characterised by high frequency and low impact; - consistency in the treatment of malicious and non-malicious acts shall be granted. Based on the following considerations: - the narrative of the scenarios proposed fully reflects the case of malicious events and they are not always applicable to non-malicious events (e.g. ransomware); - malicious attacks can be widespread whereas operational errors are hardly simultaneously happening in more than one undertaking;
GDV	Association	Overall, the approach is ok. From the perspective of immediate mitigating measures, the treatment of malicious and non-malicious in the context of a stress test is comparable. There are significant differences in the further (post-)treatment (e.g., in the context of offender investigation and prosecution).	
AAE	Association	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).	
Institut des actuarires (FR)	Association	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.	

CRO Forum	Industry	It is important to keep a consistent approach and as such paragraph 80 is a direct contradiction of this basic notion. In addition, we would like to note that despite many companies improve on internal controls and measures to avoid non-malicious events, we see a large potential for those events in the Cloud Outage scenario. This assumption is driven by what we have observed in past events. Especially in events where (only) one Cloud provider is originally causing the event, we see a non-malicious perspective as necessary. Therefore, we suggest to focus the priority of scenarios based on the impact and not on the cause (malicious vs. non-malicious). The latter could have the same or higher impact and could be considered more likely due the big chance of human error in a o lot of processes. Non malicius happens in one company hence we keep the focus on malicious. Concentration of risk and widespread events. Potential consideration ont eh underwriting and frequency. No focus on individual cases. Recommendations!!!	simultaneously happening in more than one undertaking; - an EU wide stress test exercise shall test the impact of adverse developments that affects the sector as a whole. Against these considerations, EIOPA considers the focus on malicious events as the preferred option. This will be considered also in the draft of potential recommendations which cannot be of operational nature.
METAMETRIS	Consulting	As stress tests focus on worst case impact scenarios, non-intentional events can stay outside of the scope for cyber resilience risks, they would have similar impacts as cyber attacks i.e. data compromise and/or business disruption even through in some cases the impact criticality may be lower.	
Cowbell Cyber	Industry	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. 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.	
IfoA	Association	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.	
Key assumptions	**Type**	**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.**	**Response**
Insurance Europe	Association	This question is not entirely clear as it refers to the different treatment of in-/outsource operations, while paragraph 80 refers to the (initial) lack of distinction between deliberate and non-deliberate actions. The lack of consistency creates confusion. The distinction between deliberate and non-deliberate actions would have to be considered within the context of specific examples: for many scenarios, the impact of these distinctions on observed effects could be very minor. However, the consequences will not always be the same for deliberate and non-deliberate actions. There should be further consideration regarding deliberate and non-deliberate actions, as they will have differences in: •Threat agents (internal or external) •Control sets reducing the risk •Frequency and impact •Duration •Scenarios (third party involved as attacker or as unaware entry point) A bias is not expected between in and outsourcing operational models as it is viewed that there is not a significant difference between said models	Despite diverging views from stakeholders on the distinction made on the treatment of the deliberate and non-deliberate actions on external providers, there is a common understanding on treating outsourced activities in a specific way. On the one hand, companies shall be prepared to deal with interruption of services from external providers. On the other hand, the impact can be mitigated by contractual agreements (liabilities clauses) and correctly defined and monitored SLA's. Based on the considerations below, EIOPA opts to focus on malicious events also for external providers: - interruption of services can be caused both by malicious and non-malicious acts; - malicious acts cause in general longer interruption of services which can be also spread over more than one provider; - stress test exercises shall cover severe but plausible events; - consistency of the scenarios and their application is key to grant comparability of the results.
GDV	Association	The question re. par. 80 is not entirely clear. The question refers to different treatment of in-/outsource operations, while par. 80 refers to the (initial) lack of distinction between deliberate and non-deliberate actions. Both distinctions would have to be considered within the context of specific examples - for many scenarios, the impact of these distinctions on observed effects could be very minor.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	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. 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.	
CRO Forum	Industry	We agree on the different treatment of the operational errors in case of in- and -outsource of operations. However as per paragraph 80, we disagree that the consequences will be assumed to be the same for deliberate and non-deliberate actions. We suggest that this should be separated as non-deliberate actions will have different threat agents, control sets, frequency and duration. Therefore, again, the focus should be on impact not a cause. In case of outsourced activities financial impact can be mitigated by contractual agreements (liabilities clauses) and correctly defined and monitored SLA's. In case of inhouse operations cost may be less predictable (most likely higher).	
METAMETRIS	Consulting	The question is what could be the most critical system related business disruption for a given company. In this respect a difference shall be made between companies hosting their IT on their own data centers and companies using mostly external hosting companies. In case of IT systems hosted on the company Data Centers, stress scenarios could focus on cyberattacks targeting the company DCs, in case of companies outsourcing IT infrastructure management and hosting, stress scenarios should concern service providers and in the same way as for the company itself worst case scenarios i.e. cyberattacks only could be considered. If stress scenarios are considered for both types of IT services, the impact of each type of scenarios will depend on the company risk profile. For company mostly using cloud solutions, there is a natural risk mitigation effect due to the variety of service providers that would not be targeted by a cyberattack at the same time.	
Cowbell Cyber	Industry	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.	

IfoA	Association	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.	
Key assumptions	**Type**	**What is your view on the proposed treatment of regulatory fines and compensation against legal actions? Please provide clarification.**	**Response**
Insurance Europe	Association	There is agreement that the proposed treatment of regulatory fines and compensation against legal actions should be excluded, as said measures would have to be massive to be significant. However, consideration for different local impacts means that legal actions could be a major component of the loss deriving from certain types of attacks in some scenarios.	Uncertainty, heterogeneity in national legislation and time of settlement suggest to exclude regulatory fines and compensations from a stress test exercise. However, it is recognised that the economic impact of potential legal actions can be material. Given the potential evolution of the law in this field, the regulatory fines and compensations will be included in the framework to be considered for future exercises. If included in a specific stress test exercise, the economic impact of regulatory fines and compensations will be quantified and assessed separately from the other impacts.
GDV	Association	Seems plausible.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	We should encourage local exercises.	
CRO Forum	Industry	We agree to exclude. Excluding fines and legal compensations would be an exclusion of potentially relevant impact. However, they are highly different from location to location due to various factors (including maturity of legislation and related fines), differences between primary and re-insurance and hard to quantify.	
METAMETRIS	Consulting	Regulatory fines and potential impact of client litigations should be taken into consideration in case of personal data compromise according to a cost per data subject with compromised PII. This amount could be set as a global indicator per country according to various data sources (Ponemon Institute, Verizon…).	
Cowbell Cyber	Industry	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.	
IfoA	Association	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.	
Scope	**Type**	**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.**	**Response**
Insurance Europe	Association	This will vary from group to group depending on their IT architecture. Some companies assess the concentration of crucial IT systems as part of the risk analysis for the whole financial sector performed by the authorities. In addition, the assessment of the concentration of crucial IT systems can be done through modelling techniques such as setting a high correlation (eg perfect correlation) in a dependency structure between the different modelled units, in order to account for multiple scenarios hitting simultaneously within the group (ie macro scenarios). The critical IT infrastructures listed are often shared within a group. However, there are cases where they are only shared with the largest entities in an insurance group and by extension, smaller companies often have their own critical systems as they wish to remain autonomous. If small independent entities have an interconnected IT system within the group, the risk is increased.	EIOPA takes note of the comment received and acknowledges that, even if in most cases the IT systems are shared within a group, there is still a potential heterogeneity across groups with respect to IT concentration (see resolutions to questions 8 and 9).
GDV	Association	This should be the norm for mature group companies; at least the basic infrastructure is usually provided and shared centrally. In the case of mergers, there may be transitional phases with two or more infrastructures.	
AAE	Association	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	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry	This will vary from Group to Group depending on their IT architecture. Some of our members have this centralized while others are set up in a more decentralized manner. Therefore, a one-size fits all approach will not work and an approach as adopted by EIOPA for liquidity is recommended.	
METAMETRIS	Consulting	Critical IT infrastructures can be shared within an insurance group as well as several entities of an insurance group can share the same systems from external service providers. Concentration risks expand the scope of impacted entities / processes for a single event especially for business disruption events such as ransomware attacks. Once the scope of the stress test has been defined by selecting a given worst-case scenario, the impact study will cover the impacted entities / data/ processes.	
Cowbell Cyber	Industry	The extent to which critical IT systems are shared within an IT group is outside my area of expertise.	
IfoA	Association	The extent to which critical IT systems are shared within an IT group is outside our area of expertise.	
Scope	**Type**	**Should stress testing of cyber resilience risk be carried out at group or solo level? Please provide clarification.**	**Response**
Insurance Europe	Association	Both approaches could be used, as the suitability of carrying out a cyber resilience risk on either level is determined by factors such as size, type of insurance products, and structures of process and systems, among other factors.	EIOPA welcomes the suggestions received by stakeholders with respect to the definition of the scope of the stress test. There is a general agreement that cyber resilience risk would be more appropriate to be carried out either at Group level, due to high interconnection of IT systems, or with a hybrid approach, such as the liquidity component in the EIOPA Insurance Stress Test 2021. EIOPA acknowledges the advantages of targeting Groups or of a hybrid approach. Nonetheless, the potential advantages of targeting solo undertakings are also discussed in Table 2 of the paper, which might be relevant depending on the objectives of the stress test exercise.
GDV	Association	The group view should be used (see also question 6). Breaking down into the solo companies would be very time-consuming to implement.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry	Both options could apply since there might be local differences (e.g. size, type of insurance products, legislation, expertise of processes and systems). An approach similar to taken by EIOPA on liquidity risk would be recommended.	

METAMETRIS	Consulting	To define cyber resilience stress testing scenarios at a group level, stress testing should be performed at solo level because business impact assessment can only be performed at the level of operational activities. In addition, a stress test is a worst-case scenario which can only be identified once each single entity has measured the business impact of critical cyber risks.	
Cowbell Cyber	Industry	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 inconsistencies to ensure that there is a 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.	
IfoA	Association	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.	
Scope	**Type**	**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.**	**Response**
Insurance Europe	Association	There is no one-size-fits-all approach and there is not an approach that will make sense in all cases. Therefore, both approaches could be considered as the way that solos and groups would be impacted depends on several factors as described in questions 7 and 8.	EIOPA acknowledges the support shown towards a hybrid approach to the scope definition. It also takes note on the views that an aggregation at Group level should always be done, even if the exercise is designed at solo level. Regarding the views that the scope should be decided by the participants, although acknowledging the arguments presented by stakeholders, this could lead to a heterogeneous application of the exercise at European level, and it might jeopardize the conclusions of the exercise. Moreover, defining the scope of stress test exercises carried out at European level is a task of EIOPA as defined in its governing Regulation (Art. 32, 2(b)), in collaboration with NCAs.
GDV	Association	This approach seems to be comprehensible for us, especially if not every Solo undertaking is exposed to cyber underwriting risk.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	Local and business-specific solo visions are essential. An aggregation of the results at group level is necessary, taking into account the propagation and extension effects between entities.	
CRO Forum	Industry	As per Q& and Q8, for both the resilience test and the cyber underwriting test, it is critical that the participants have the options to participate either at group level or at local level. Both options could apply since there might be local differences (e.g., size, type of insurance products, legislation, expertise of processes and systems). An approach similar to taken by EIOPA on liquidity risk would be recommended.	
METAMETRIS	Consulting	Cyber resilience risks at a group level implies to limit risk assessment to the largest infrastructure or service providers of a group which can be complex to define before any impact assessment, in addition risk assessment should be performed for all entities having access to this infrastructure. In our opinion the best approach to cyber resilience stress testing even at Group level is to perform the stress testing at solo level and then select a worst case stess scenario at Group level. In addition stess scenarios can be assessed for group infrastructures at single entity level.	
Cowbell Cyber	Industry	Appropriate, for the reasons described in answers to Q's 7 and 8.	
IfoA	Association	Appropriate, for the reasons described in answers to Q's 7 and 8.	
Scope	**Type**	**Which are in your view the Solvency II lines of business expected to be more impacted by affirmative cyber underwriting risk?**	**Response**
Insurance Europe	Association	Affirmative cyber underwriting risk is expected to have an impact on various lines of business due to the variety of perils covered by cyber insurance contracts. From a Solvency II perspective, the main lines of business that are impacted are: •General liability (direct and proportional), •Legal expenses (direct and proportional) and •Non-proportional casualty •Fire and other damage to property insurance •Miscellaneous Financial Loss •Assistance (direct and proportional).	EIOPA welcomes the input of stakeholders and will consider it in future exercises. According to the answers received, the Solvency II lines of business expected to be more impacted by affirmative cyber underwriting risk are Fire and other damage to property insurance, General liability insurance, Miscellaneous financial loss (mainly Business Interruption). Other least mentioned business lines, but still relevant, are Legal expenses insurance and Assistance. These references are now added to the paper.
GDV	Association	It would be either Property or Liability or Miscellaneous Financial Loss.	
AAE	Association	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	
Institut des actuarires (FR)	Association	Civil Liability & business interruption.	
CRO Forum	Industry	Solvency II Lines of business that would be most impacted by affirmative cyber underwriting risk are: LoB 7 (Fire and other damage to property insurance) and LoB 8 (general liability). LoB 10 (legal & protection) and LoB 12 (financial loss incl. Business Interruption) could also be impacted.	
METAMETRIS	Consulting	Non-life liability and damage insurance.	
Cowbell Cyber	Industry	9. Other damage to property 13. General liability 16. Miscellaneous financial loss	
IfoA	Association	9. Other damage to property 13. General liability 16. Miscellaneous financial loss	
Scope	**Type**	**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)?**	**Response**

Insurance Europe	Association	Due to its implicit nature, non-affirmative cyber underwriting risk can have a material indirect impact to the following Solvency II lines of business: •Fire and other damage to property (direct, proportional, non-proportional), •Marine, aviation and transportation (direct, proportional, non-proportional), •General liability (direct and proportional), •Credit and suretyship (direct and proportional), •Legal expenses (direct and proportional), •Non-proportional casualty.	EIOPA welcomes the input of stakeholders and will consider it in future exercises. According to the answers received, the Solvency II lines of business expected to be more impacted by non-affirmative cyber underwriting risk are Fire and other damage to property insurance, General liability insurance, Legal expense insurance and Miscellaneous financial loss. Other mentioned business lines are Marine, aviation and transport insurance, and Credit and suretyship insurance. Motor vehicle liability insurance was also mentioned. These references are now added to the paper. It is also mentioned by stakeholders that the non-affirmative cyber underwriting risk will tend to decrease with time due to the work that is currently being done in order to clarify cyber exclusions. This is now mentioned in paragraph 66 of chapter 2.
GDV	Association	For primary insurance business, affected lines are fire and other damage to property as well as general liability. For reinsurance business, the mainly affected lines of business with regard to cyber risk are property and casualty business, as well as general liability. As the development and adoption of cyber exclusions is already rather mature for property, we expect casualty to be the main driver here. But we can already see exclusions being applied more and more in casualty as well, so in the near future marine insurance might become more relevant due to a lack of market wide acceptable exclusion clauses that are actually deemed effective. In general, the risk of silent cyber coverages is becoming smaller every year due to the successful implementation of exclusions such that with timelines of business with little exposure will take the lead in overall exposure because of the lack of focus on exclusions.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	Civil Liability & business interruption.	
CRO Forum	Industry	Solvency II Lines of business that would be most impacted by non-affirmative cyber underwriting risk are: 7 (fire & other damage), 8 (general liability) 10 (legal & protection) et 12 (financial loss incl. business interruption)	
METAMETRIS	Consulting	Non-life liability and damage insurance.	
Cowbell Cyber	Industry	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 13. General liability 15. Suretyship 16. Miscellaneous financial loss	
IfoA	Association	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	
Scope	**Type**	**What is your view on the criteria for the selection of the participating entities listed in Table 3? Please provide clarification.**	**Response**
Insurance Europe	Association	The scope for the table would be expected to be set in accordance with the effect in the event of a failure, rather than the size of the market or business. For the cell pertaining to exposure and cyber resilience, risk profile should be included with size of the company. The use of "critical functions" to determine scope of a cyber stress test is not supported and should be avoided, particularly at the present time given its importance in the ongoing discussions on the EC's Insurance Recovery and Resolution Directive proposal	EIOPA notes the general consensus on the criteria and metrics proposed. EIOPA also welcomes some of the suggestions received (see resolution to question 13). Regarding the use of the terminology "critical functions", EIOPA does not see it as hampering the ongoing discussion on a EU widely accepted definition of critical functions in the context of the IRRD negotiations. The concept of "critical functions" as used in the paper is based on the IAIS definition and it is aligned with the approach of EIOPA's paper on "Systemic risk and macroprudential policy in insurance", as appropriately indicated in the paper: https://www.eiopa.europa.eu/system/files/2019-03/syssystemic_risk_and_macroprudential_policy_in_insurance.pdf. The EIOPA EU-wide stress test exercises aim at assessing the resilience of the insurance insustry against specific scenairos, e.g. adverse economic and markets developements, climate, liquidity. Stress test exercises cannot target all the european insurance undertakings, a subset of them, considered representative for the industry is identified following criteria based on exposure to the specific scenarios, relevance for the Europen / local markets, and potential systemic relevance. The framework at stake shares the same principles. While aiming at assessing the resilience of the
GDV	Association	For primary insurance we agree with the proposed criteria. For reinsurance business, the following applies: While the size of the portfolio written in nonlife is certainly a key metric to assess the general exposure to silent cyber, it ignores the effort of undertakings to include exclusions. At the same time, a percentage of contracts in place per line of business without exclusion is probably not a metric that can be provided. With regard to measuring the exposure for affirmative cyber risk, we suggest to focus on the size of standalone cyber coverage provided. While add-on policies are typically much larger in numbers, they usually provide only very little coverage and thus the risk behind these types of coverages is very limited and not comparable to standalone cyber exposure.	
AAE	Association	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 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	
Institut des actuarires (FR)	Association	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).	

CRO Forum	Industry	Criteria for the selection of the participating entities listed in Table 3 are okay. Furthermore, we disagree with the use of the concept of "critical functions" as a criterion for the purpose of the cyber stress tests. The EIOPA paper resorted to an IAIS definition in footnote 48 because there is no EU legal definition of this concept at present, and it is in the remit of the EU legislators to provide one as part of the IRRD negotiations. The concept of 'critical function' is mostly relevant in the context of resolution, i.e., where insurers failed or are likely to fail, for the public interest test. For going concern exercises such as stress testing, this concept is not an appropriate criterion.	shares the same principles. While aiming at assessing the resilience of the insurance industry and of its members, the participants in the exercise are identified based on their exposures to the ientified scenarios, and their relevance for the European financial system.
METAMETRIS	Consulting	For cyber resilience risk various size criteria can be considered to define selected entities, but turnover metrics may not be homogeneous between the various business lines (i.e non-life, life and asset management). The number of headcounts may be a good size indicator which is in addition highly correlated with potential impact of a business disruption.	
Cowbell Cyber	Industry	Agreed.	
IfoA	Association	Agreed.	
Scope	**Type**	**Are there any other relevant criteria not covered in Table 3 or in your answers to the previous questions? Please specify.**	**Response**
Insurance Europe	Association		EIOPA welcomes the suggestions received by stakeholders on the selection of undertakings. In principle, size-based and risk-based metrics are already included and the granularity might be enhanced based on the information that will become available with the Solvency II reporting review. With regards to cyber resilience, the number of employees (e.g. headcounts) was added as an additional metric in Table 3. Finally, while agreeing on the potential utility of additional metrics on cyber resilience, such as external cyber scores, EIOPA prefers to rely on information collected via Solvency II processes to ensure their robustness.
GDV	Association		
AAE	Association	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.	
Institut des actuarires (FR)	Association	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).	
CRO Forum	Industry	No	
METAMETRIS	Consulting	For cyber resilience risk the number of personal data subjects within company data bases is highly correlated with the potential impact of massive data exfiltration.	
Cowbell Cyber	Industry	No	
IfoA	Association	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.	
Scenarios	**Type**	**What is your view on the five selected scenarios for both cyber underwriting and cyber resilience risks? Please provide clarification.**	**Response**
Insurance Europe	Association	In terms of the design of cyber stress tests, it is important to recognise the fact that the market in question is maturing and remains highly specialised. As such, any European stress tests will come at a critical time and be influential on the development of the market, including by potentially having an effect on both regulatory and industry considerations and approaches. It would, therefore, be desirable for EIOPA to further consult on specific scenarios once these have been designed in full as, although it is also very helpful to provide input to the high-level design principles at this stage, important facets may emerge in detailed scenario designs which would merit industry input, and which would not be apparent at the design stage. Nevertheless, and until a detailed consultation is carried out by EIOPA, some preliminary points on the scenarios are provided: •The data centre/infrastructure (cloud outage) damage scenario is a problem specific to a specific insurance company, whereas the power outage scenario is a global risk by territory. Thus, data centre/infrastructure damage would imply a reputational risk that power outage would not. •The data centre/infrastructure (cloud outage) damage scenario is usually not the consequence of a cyber act, but rather the consequence of an event (such as a natural disaster) affecting IT infrastructures. Nonetheless, it is a relevant scenario as there may be severe consequences, especially if infrastructures are shared across a group and there is an additional cost for policyholders to check data and systems to ensure that they have not been corrupted. The cloud outage underwriting scenario could benefit from having additional dimensions included in the scenario design principles. For example: the outage timeframe (eg hours/days), what is impacted (eg major cloud service provider) and what was the cause (eg misapplied software attacked by malicious code). •With additional regard to power outage, the scenario itself is seen as very impactful, but not necessarily as part of a cyber stress. Power outages can have many sources, with cyber being only one among many - and a very unlikely one compared to others at that. Furthermore, it can be complicated to define and calibrate, as it is understood to concern an energy-operator failure. •There could be a connection between ransomware and data breach, as both scenarios have closely related risks and consequences. It is noted that they do not systematically occur together, but there are some instances where the data unavailability caused by a ransomware attack can fall under the case of a data breach. •Denial of service is, in general, not deemed significant. For most insurers and pension providers, an outage would need to be of a long duration to be significant. "Simple" denial-of-service attacks can usually be mitigated rather quickly. The denial-of-service underwriting scenario could benefit from having additional dimensions included in the scenario design principles. For example: who is impacted (eg global IT network of a MNE), whether it includes a ransom demand, length of outage (eg hours/days), location (national/regional/global). Generally, it is reasonable to estimate financial impacts for the given scenarios as part of a EIOPA stress testing exercise. However, conducting and documenting business interruption exercises - with details of qualitative information such as the availability of backup systems - should not part of such a stress test. Further, this type of information will presumably be available via the tests implemented in the Digital Operational Resilience Act (DORA). Summarising the above-mentioned arguments, it is advised that EIOPA carries out a detailed consultation on the specificities of each scenario. Until this takes place, it is concluded that the ransomware, cloud outage and data breach scenarios are relevant and necessary; denial of service is deemed to be comparatively small but still a valid scenario; whereas power outage does not seem to fit a cyber stress testing framework in its current wording.	EIOPA takes note of the relevance of the proposed scenarios, which will be considered in designing specific exercises. As mentioned in the discussion paper, the list of proposed scenarios is not exhaustive, additional scenarios might be developed. Moreover, as for the past EIOPA stress tests, scenarios and specifications will be subject to discussion and consultation with the industry and the participants before the launch of the exercisce. While agreing that technical information on the IT infrastructure and back-up systems shall be potentially reported under DORA, being a cyber exercise never run before, EIOPA still aims at collecting qualitative ancillary information to explain and justify potential impacts on the insurers against the specified events and to gain experience on the topic. The scenario definitions are based on an impact perspective, while leaving the exact attack vector open on purpose. This is as to keep the scenario applicable for a wide range of IT-infrastructures that might be in place at the diverse undertakings of the insurance sector. For this reason, scenarios based on more specific attacks such as a 'logic bomb' or an infection over a third party will not be explicitly included in the framework at this point. EIOPA opted not to include the unauthorised transaction scenario because this type of event is unlikely to be orchestrated simultaneously in more than one organization, hence it is not suitable for EU-wide stress testing.

GDV	Association	Generally, it is reasonable to estimate financial impacts for the given scenarios as part of a EIOPA stress testing exercise. However, conducting and documenting business interruption exercises - with details of qualitative information such as the availability of backup systems - should not part of such a stress test. Further, this type of information will presumably be available via the tests implemented in DORA. For cyber underwriting, coverage for cloud outage is oftentimes only added to standalone covers on an add-on basis or excluded entirely. In combination with the provided reasoning with regard to likelihood and impact, this should not be a main scenario. At the moment, the ransomware scenario would be our main concern and we would expect this scenario to have the biggest impact. The scenario DoS is not as relevant anymore for the undertaking itself in our opinion, as you suggested, the main problem is a service provider outage which in turn might be due to different scenarios, not just DoS. We therefore suggest to base the scenario on ""service provider outage other than cloud"" rather than DoS. Data breach is another very relevant scenario based on our findings. We see this as the second most central one besides ransomware. With regard to power outage we see the scenario itself as very impactful, but not necessarily as part of a cyber stress. Power outages can have many sources, cyber is only one among many and a very unlikely one compared to others at that. We therefore do not think that this scenario should be included in a cyber stress testing framework. Combining the above mentioned arguments, we conclude that the ransomware and data breach scenarios are relevant and necessary, the cloud outage scenario is comparably very small but still makes sense whereas the scenarios DoS and power outage do not seem to fit a cyber stress testing framework in their current wording.	
AAE	Association	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. 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.	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry	The "Ransomware" scenario should rather be considered in a broader "malware" scenario (e.g. to also wiper events). We also question if cloud outage is included in the DC scenario why do we have a separate scenario for power outage? Furthermore, for underwriting except for property damage there is no difference between power outage and cloud outage. We would therefore suggest to remove the power outage scenario, which is a typical operational risk scenario but not one based endogenously on cyber security issues.	
METAMETRIS	Consulting	For cyber resilience risk the selected scenarios seem to be generic enough to reflect the exposure to the most critical cyber & IT risks.	
Cowbell Cyber	Industry	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. Scenario 2 is cyber resilience if it is a ransomware attack against the insurer itself and underwriting if on an insured. 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 perspective. 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.	
IfoA	Association	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.	
Scenarios	**Type**	**Which scenario do you consider most relevant from the list of scenarios proposed for cyber underwriting? Please provide clarification.**	**Response**
Insurance Europe	Association	ansomware (and other types of destructive cybercrime) is considered the most relevant for cyber underwriting as it is the scenario which costs the most for companies, especially if it comes with a data breach. Furthermore, it is relevant due to the global proliferation of attacks and the uncertainty in the approach taken by insurers on whether to insure such attacks. In addition to ransomware, cloud outage is a significantly relevant scenario. These scenarios are relevant as they could have a large impact, be widespread, and the severity could be high	EIOPA takes note of the stakeholders' assessment of the relevance of the different scenarios. This will be considered when developing a stress-test exercise. Some stakeholders comment that power outage is often excluded for silent

GDV	Association	see question 14: ransomware based on observed losses	cyber. However, EIOPA considers that in the case of non-affirmative cyber, power outage can still have an impact on the claims cost.
AAE	Association	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.	
Institut des actuarires (FR)	Association		
CRO Forum	Industry	Cloud outage and ransomware/malware scenarios are more relevant as they would have a large impact, widespread, and high severity.	
METAMETRIS	Consulting	In our opinion ransomware targeting a systemic risk provider would be the worst case scenario for an cyber insurance portfolio.	
Cowbell Cyber	Industry	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 eg cybersecurity practices	
IfoA	Association	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	
Scenarios	**Type**	**Which scenario do you consider most relevant from the list of scenarios proposed for cyber resilience? Please provide clarification.**	**Response**
Insurance Europe	Association	Ransomware, cloud outage and data breach (and other types of destructive cybercrime) are considered to be the most relevant for cyber resilience. In addition, they may cause availability and confidentiality issues that organisations might face that are linked to a number of causes.	EIOPA takes note of the responses received and these will be considered when developing a stress test exercise. Ransomware and Data Breach are clearly considered to be the most relevant by stakeholders. It is also pointed out that, depending on the circumstances, all the proposed scenarios can be relevant to an undertaking.
GDV	Association	Data breach + Ransomware are deemed to have the highest operational impact within current scenarios considered	
AAE	Association	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.	
Institut des actuarires (FR)	Association		
CRO Forum	Industry	All named scenarios can be relevant. Which one is most relevant differs from company to company.	
METAMETRIS	Consulting	For cyber resilience risk the scenarios ransomware and data breach, in isolation or combined are generic and could well reflect the worst-case scenarios.	
Cowbell Cyber	Industry	Scenario 2 "Ransomware / Data Theft" is the most likely event to occur and thus the most important to test for resilience	
IfoA	Association	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.	
Scenarios	**Type**	**Are there any additional cyber risk stress scenarios that should be considered? If yes, please provide their narrative and specification.**	**Response**
Insurance Europe	Association		EIOPA takes note of the responses received. The scenario definitions are based on an impact perspective, while leaving the exact attack vector open on purpose. This is as to keep the scenario applicable for a wide range of IT-infrastructures that might be in place at the diverse undertakings of the insurance sector. For this reason, more specific attacks such as a 'logic bomb' or an infection over a third party as suggested, will not be included in the framework at this point. Fraudulent transactions, as reported in the resolution to the question on scenarios (Q.14) does not fully qualify as a stress test event.
GDV	Association		
AAE	Association	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).	
Institut des actuarires (FR)	Association		
CRO Forum	Industry	No	
METAMETRIS	Consulting	Other types of cyber scenarios can be considered for risk mitigation purpose but selecting a limited number of scenarios such as ransomware and data breach would provide consistency across the industry.	
Cowbell Cyber	Industry	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.	
IfoA	Association	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.	
Scenarios	**Type**	**What is your view on the separate treatment of the Ransomware and Data breach scenarios? Please provide clarification**	**Response**
Insurance Europe	Association	For cyber underwriting, this separation can be very helpful with regard to the application to different types of coverage. As many policies differentiate between first- and third-party coverages, it seems to be sensitive to mirror that distinction in the scenarios (ransomware being mainly first party driven and data breach being a scenario for third party coverages). In addition, ransomware and data breach do not systematically occur together. Regarding cyber resilience, the distinction seems necessary, as the motive behind undertaking a ransomware attack or data breach attack would be different.	EIOPA takes note of the comments received which clearly favour the separate treatment of Ransomware and Data breach scenarios. Against this background, EIOPA keeps Ransomware and Data breach as distinct scenarios.
GDV	Association	For cyber underwriting, this separation can be very helpful with regard to the application to different types of coverage. As many policies differentiate between first- and third-party coverages, it seems to be sensitive to mirror that distinction in the scenarios (Ransomware being mainly first party driven and data breach being a scenario for third party coverages). Regarding cyber resilience, the distinction seems necessary	
AAE	Association	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.	
Institut des actuarires (FR)	Association		
CRO Forum	Industry	We agree to split the scenarios as they're not mutually exclusive, do not systematically occur together and have a different impact on the organisation and what recovery actions are required. Data breach may be a consequence of the ransomware and vice versa, so some factor of correlation may exist.	
METAMETRIS	Consulting	The separate treatment of ransomware and data breaches makes sense as their impact study is very different (even though they can be combined in a single event) and the extreme materialization of both types of events can base on different attack types (see Mitre Att&ck). However, it should be a decision of the industry to combine or separate the two stress tests by calibrating their correlation level.	
Cowbell Cyber	Industry	Data breach could be dropped as extortion through disruption and data theft is prominent and covers the data breach risk.	
IfoA	Association	Data breach could be dropped as extortion through disruption and data theft is prominent and covers the data breach risk.	
Cyber Underwriting: Shocks, Specifications and Metrics	**Type**	**What is your view on the proposed metrics and indicators in terms of completeness and viability? Please provide clarification.**	**Response**

Insurance Europe	Association	The provisions, claims and loss ratio metrics are relevant. The output metrics are suitable, as they are the ones present in Solvency II. The "cyber loss ratio" metric is difficult to compute in an isolated manner, as of today	Stakeholders generally agreed with the metrics proposed, with the following restrictions: - The "cyber loss ratio" will be difficult to compute; - The data availability may be reduced for reinsurers; - For non-affirmative cyber risk, the impact is difficult to measure quantitatively. Nevertheless, EIOPA considers that these elements should not be excluded in advance. Further clarification will be provided in the "Technical Specifications". To address the concerns related to the loss ratio, changes have been made in the paper regarding the metric "Loss ratio for (affirmative and non-affirmative) cyber products" (table 11). A joint reporting for affirmative and non-affirmative cyber risk is now proposed to avoid the problems of unknown premiums for silent cyber. Some respondents proposed to remove the metric "change of assets" in table 11 since this may not be related to underwriting risk. The metric is kept due to its relevance to assess the impact of direct pay-out of claims (e.g. through a variation of cash) or of reinsurance (through a variation of the recoverables). Further clarification has been added.
GDV	Association		
AAE	Association	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.	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry	We have a variety of observations from our members: The "cyber loss ratio" metric is difficult to compute in an isolated manner as of today for several of our members. For non-affirmative coverage, a more qualitative approach is likely to be more appropriate and informative as, by design, the cyber risk driver is not quantitatively isolated. The CRO Forum agrees with EIOPA (cf. para 136) that participants should have the flexibility, depending on the scenarios and the type of business being impacted, to reflect the impacts of the shocks either through a change of reserves, through a change/depletion of cash, or through both. No prescription should be set out here in line with the proportionality principle. To avoid any confusion, the proposed metric "change of assets" should be amended into "change of cash". Finally, as explained in the general comments, the CROF disagrees with a re-calculation of the SCR post-shock or to add impacts at the level of Solvency II eligible own funds. EU stress tests should test the build-up of macro financial stability risks in the single market, and not second guess the Solvency II ratio.	
METAMETRIS	Consulting	The number of headcounts within portfolio companies is needed to measure recovery expenses. Loss of profit bases on new business turnover.	
Cowbell Cyber	Industry	No comment	
IfoA	Association	No comment	
Cyber Underwriting: Shocks, Specifications and Metrics	**Type**	**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.**	**Response**
Insurance Europe	Association	Depending on the LoB, it is reasonable to distinguish between affirmative and non-affirmative cyber risk. As mentioned above, the industry sees problems with regard to the differentiation between the two types of add-on coverage. With regard to the differentiation between silent cyber and affirmative cyber risk, in general, the industry sees this as a key difference that should absolutely be reflected in the reporting. There is a profound difference between the metrics for silent and affirmative exposure and the industry finds these numbers should not be mixed. 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. This is especially the case, as the peril is constantly subject to change and hence changes in affected lines of business and types of coverage are to be expected.	Stakeholders largely agree with splitting metrics for affirmative and non-affirmative coverages. Nevertheless, the following challenges are identified: - to assess the impact on non-affirmative coverages; - to distinguish between the two types of add-on coverage for affirmative coverage. EIOPA considers that these aspects should not be excluded in advance. Data limitations can be taken into account in the Technical Specifications, can be complemented by the submission of qualitative information, and will be made transparent in the final report. Some comments highlight that the computation of the loss ratio for non-affirmative cyber may not be possible because the cyber premium is not known. Changes have been made in the paper regarding the metric "Loss ratio for (affirmative and non-affirmative) cyber products" (table 11). A joint reporting for affirmative and non-affirmative cyber is now proposed to avoid the problems of unknown premiums for silent cyber.
GDV	Association	Depending on the LoB it is reasonable to distinguish between affirmative and non-affirmative cyber risk. As mentioned above, we see problems with regard to the differentiation between the two types of addon coverage. With regard to the differentiation between silent cyber and affirmative cyber risk, in general, we see this as a key difference that should absolutely be reflected in the reporting. There is a profound difference between the metrics for silent and affirmative exposure and we find these numbers should not be mixed. 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.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	Non affirmative coverages cannot be part of the stress tests.	
CRO Forum	Industry	This is feasible if approximations may be used (e.g. for some members on the non-affirmative part).	
METAMETRIS	Consulting	It seems extremely complex to define metrics to model non affirmative coverage without detailed specification on exposure at industry level.	
Cowbell Cyber	Industry	For non-affirmative, the portion being allocated to cyber perils varies significantly between insurers. This may require narrative to better differentiate the submissions.	
IfoA	Association	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.	
Cyber Underwriting: Shocks, Specifications and Metrics	**Type**	**What is your view on the feasibility of the metric "Expected losses if key exclusions are not applicable under stress"? Please provide clarification.**	**Response**
Insurance Europe	Association	As uncertainties exist, the industry agrees that expected losses should be consistent 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 a simultaneous failure of all is not a realistic basis for a shock. So, the extent and the impact of non-applicable exclusions should be concretized. In addition, expected losses if reinsurance is not responding as expected should be considered. This is especially important to non-affirmative covers, as reinsurance exclusions are oftentimes stricter than insurance exclusions and, therefore, do not offer back-to-back coverage.	Several stakeholders point out that EIOPA should describe precisely what is meant by "key exclusions are not applicable under stress". EIOPA agrees that this precise description has to be included in the Technical Specifications in any future stress test exercise with focus on cyber risk. However, since this description depends on the narrative of the chosen scenario, it cannot be included in this Methodological paper. Additionally, responses note that the variety of exclusion clauses is large and that it is not likely that they will all not be applicable. The aim of the proposed metric is to capture the materiality of potential legal risk
GDV	Association	As uncertainties exist, we agree that expected losses if exclusions are not applicable should be considered. Nevertheless, the variety of existing exclusions, even of the most widely used ones, is large. The schematics of the exclusions differ so much that a simultaneous failure of all is not a realistic basis for a shock. So the extent and the impact of non-applicable exclusions should be concretized. In addition, expected losses if reinsurance is not responding as expected should be considered. This is especially important to non-affirmative covers as reinsurance exclusions are oftentimes stricter than insurance exclusions and therefore do not offer back-to-back coverage.	

AAE	Association	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.	associated to exclusion clauses. A clarification is now added in the paper (see Methodological paper, par. 154). Finally, EIOPA takes note of the comments highlighting that reinsurance might not respond as expected. According to stakeholders, reinsurance exclusions for non-affirmative covers are often stricter than insurance exclusions and therefore do not offer back-to-back coverage.
Institut des actuarires (FR)	Association	It is feasible and necessary (e.g. Definition of Cyberwar).	
CRO Forum	Industry	We do not support. It's not possible to properly and clearly define, as otherwise an evaluation would be based on many vague assumptions or just lead to the reporting of full limit losses across the entire book of the companies.	
METAMETRIS	Consulting	Per definition expected loss is null for stress scenarios.	
Cowbell Cyber	Industry	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.	
IfoA	Association	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..	
Cyber Underwriting: Shocks, Specifications and Metrics	**Type**	**What is your view on the approach to silent cyber approximation? Please add suggestions to improve it and provide clarification.**	**Response**
Insurance Europe	Association	The approach can be regarded as pragmatic and comprehensible, but could lead to uncertainties and imprecise results. For reinsurance undertakings, the application of the proposed example shocks might lead to roughly estimated results as much of the required information is not available to them. In general, numbers for silent cyber should not be expected to be available in as much detail as for affirmative cover.	Stakeholders generally agree with the proposed approach, but some question whether the impact of silent cyber can be evaluated accurately. EIOPA agrees that it is challenging to assess the impact on non-affirmative coverages. Nonetheless, non-affirmative coverages should not be excluded from the analysis in advance. Comparability of results is important. Therefore data limitations can be taken into account in the Technical Specifications, can be complemented by the submission of qualitative information, and will be made transparent in the final report. To reflect the potentially reduced availability of information for reinsurance companies in certain areas, simplified templates might be used for these undertakings (see Methodological Paper, par. 152).
GDV	Association	The approach can be regarded as pragmatic and comprehensible but could lead to uncertainties and imprecise results. For reinsurance undertakings, the application of the proposed example shocks might lead to roughly estimated results as much of the required information is not available to them. In general, numbers for silent cyber should not be expected to be available in as much detail as for affirmative cover.	
AAE	Association	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).	
Institut des actuarires (FR)	Association	Silent cyber cannot be correctly evaluated therefore we do not support the approach to silent cyber approximation.	
CRO Forum	Industry	We support the approach, with the caveat that the proxies listed in the document are just examples and that further or different proxies could be used depending on the needs (please note our general comment on e.g. differences between insurers and re-insurers).	
METAMETRIS	Consulting	Defining the scope of insurance products exposed to non-affirmative cyber risk seems complex and requires industry wide specification.	
Cowbell Cyber	Industry	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.	
IfoA	Association	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.	
Cyber Underwriting: Shocks, Specifications and Metrics	**Type**	**What is your view on the data collection? Is there any relevant information missing? Please provide clarification.**	**Response**
Insurance Europe	Association	There is agreement on the general scope of the data collection, but consideration should be taken on a few aspects: •It is becoming more and more common to insert sub-limits or exclude certain parts of typical coverages. Thus, this should be included as it has a huge impact on the risk. These would need to be applied on a more granular level. •It must be taken into account that data of non-affirmative cyber exposure is only available to a certain extent. •Table 9.4.3 in the annex is not feasible, as there is not an exhaustive view of all IT service providers used by clients covered by an insurance policy.	Several responses state that it might not be possible to identify all service providers as described in the example template 9.4.3 of the Discussion paper. Nevertheless, this information is relevant to assess potential concentration risk and should not be excluded a priori. The table is therefore kept in the methodological paper. Furthermore, respondents suggest to take into account that in the event of a cyber claim involving more than one guarantee, the contractual conditions usually provide the application of an overall coverage limit that could be significantly different than the sum of the individual limits associated with each guarantee. Therefore, the overall exposure of a company to affirmative cyber risk cannot be calculated as the sum of the exposure of the individual lines of business, as the latter would return an outstanding amount substantially higher than the real exposure. This aspect is noted and will be considered in the templates for the reporting of the metric "Exposure". The way the undertaking calculates the exposure (Sum Insured, Effective Sum Insered, Probable Maximum Loss etc.) should be in line with
GDV	Association	We agree with the scope of the data collection. However, it is becoming more and more usual to insert sublimits or exclude certain parts of typical coverages. Thus, this should be included as they have a huge impact on the risk. These would need to be applied on a more granular level. In addition, it has to be taken into account, that data of non-affirmative cyber exposure is only available to a certain extent.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	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.	

CRO Forum	Industry	We note various challenges at the moment with the data collection that need further consideration. For example, on non-affirmative, not all our members will be able to provide the Technical Provisions (TP) related to cyber risk specifically. Also, a split by "guarantee" in terms of cost component may not be available. Furthermore, table 9.4.3 is not feasible as our members do not have the exhaustive view of all IT services providers used by our clients covered by a cyber insurance policy.	the exposure management.
METAMETRIS	Consulting	See 19	
Cowbell Cyber	Industry	I think narrative discussing key assumptions made in the approach will be important.	
IfoA	Association	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.	
Cyber Resilience: Shocks, Specifications and Metrics	**Type**	**What is your view on the assumed increase in operational and other costs due to a cyber risk event? Please provide clarification.**	**Response**
Insurance Europe	Association	There is an agreement on the assumed increase in operational and other costs due to a cyber risk event. In particular, recovery costs could be significant.	EIOPA takes note of the general agreement with the proposed approach, as evidenced by the responses received. With regards to the potential interactions with DORA, EIOPA considers that the concept of stress test complements DORA requirements. In potential future cyber stress test exercises, alignment in the terminology will be granted once the policy deliverables under DORA are finalised.
GDV	Association		
AAE	Association	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.	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry		
METAMETRIS	Consulting	Increased operational costs are significant in case of major business disruption. To measure the impact of business disruption on operational cost the key indicator is the duration of the event that can be estimated by the IT team. The estimation of the resulting cost can base on a percentage of the daily salaries of impacted headcounts multiplied by the duration. 50% can be an approximation of this percentage as at a given day only 80% of staff work and for some staff especially sales people lost working days will not be compensated but result in loss of turnover. In case of loss of data, the cost of data reconstruction has to be measured separately.	
Cowbell Cyber	Industry	I agree with the method of allowing for these but when allowing for these, a default option should be provided with participants encouraged to estimate the costs themselves and provide narrative to support any deviation.	
IfoA	Association	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.	
Cyber Resilience: Shocks, Specifications and Metrics	**Type**	**What is your view on the proposed shocks in terms of completeness? Please provide clarification.**	**Response**
Insurance Europe	Association	The list of proposed shocks seems exhaustive. Some additional comments are proposed to limit the scope: •For the data breach scenario, the concepts of "data breached" and "sensitive data breached" should be merged to consider a worst-case scenario: ie only "sensitive data breached". •For the "cloud outage" scenario: the "outage time" should be considered only for critical functions as defined in DORA. •When considering data lock scenarios (eg ransomware), stressing the number of business processes affected may result in an unrealistic scenario. Based on the own process of business continuity management, the relationship between assets and business processes involved is known in theory.	EIOPA takes note of the general agreement with the proposed shocks and of the suggestions to further improve their specification. In particular: - for the data breach scenario, EIOPA will consider only "sensitive data breached" to capture the worst case scenario; - for the cloud outage scenario, in the assessment of cyber resilience, the outage time should be applied to the core applications and databases supporting business operations of the undertaking, which might coincide, but not be limited to the list defined in DORA. Further considerations might be done in the design phase of a potential cyber stress test exercise.
GDV	Association	The list of proposed shocks seems exhaustive. Regarding data breach, it is unclear if this refers only to loss of confidentiality (data are still available to us but external party obtains access/copies) or if we lose access to the data (see 237 - ""restore records breached"")	
AAE	Association	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.	
Institut des actuarires (FR)	Association	The proposed shocks seem to us to be relatively complete, even if it seems difficult to anticipate all the possible shocks that could occur.	
CRO Forum	Industry	In terms of 'completeness' it may be fine, however, on the details we would like to request EIOPA to consult any actual draft scenarios and specifications before an exercise with industry for sense-checking and practicability review. For example, although theoretically interesting, the 'percentage of data breached' approach is in our view not very practicable. Similarly, the scope of a data breach needs to be well defined within a scenario.	
METAMETRIS	Consulting	For the scenarios in table 16 the following shocks could be considered: -Duration of outage in number of days (below one day in the insurance industry the impact is not significant), -Duration of loss of data in transaction data bases, -Number of headcounts of the affected business processes, -Daily new business turnover (or NBV according to regulator's choice) of the affected business processes, -Number of compromised records of personal data subjects. The percentage of data breached doesn't mean much and doesn't allow a direct estimation of the impact, it could be replaced by the number of records concerning personal data subjects. The cost of data breach per personal data subject could be computed at industry and country level and include legal proceedings regulatory fines, etc.	
Cowbell Cyber	Industry	The proposed shocks are materially complete. However, the impact of the shock will need greater guidance to ensure consistency in estimation.	
IfoA	Association	The proposed shocks are materially complete. However, the impact of the shock will need greater guidance to ensure consistency in estimation.	
Cyber Resilience: Shocks, Specifications and Metrics	**Type**	**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.**	**Response**

Insurance Europe	Association	Yes, there is the agreement that the shocks are provided in technical terms, such as the duration of the outage. However, these technical terms must be able to measure the real impact on the ability of the organisation to fulfil its function. Also including monetary measures is a good way of doing this, as the risks are more comparable in this format	EIOPA takes note of the broad agreement to consider cyber resilience shocks in technical terms rather than in terms of financial costs as the latter derive from the former and are likely institution-specific. EIOPA also acknowledges the difficulties inherent to the potential estimation of financial costs and therefore, in the event of a future stress test exercise with focus on cyber risk, EIOPA could consider to provide shocks also in terms of financial costs as a benchmark whenever participants cannot estimate these on their own. For the calibration of such shocks, EIOPA could engage in collaboration with other European agencies or platforms (e.g. ESRB, ENISA, Joint Cyber Unit), practitioners, academia and model vendors. This is now clarified in the paper.
GDV	Association	Yes, we agree.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	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, 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).	
CRO Forum	Industry	We agree that shocks are provided in technical terms such as duration of outage. However, these technical terms must measure- the real impact on the ability of the organization to fulfil its function. Several members consider it more appropriate and accurate to derive their own financial costs based on EIOPA technical shocks, whereas for other members it could be helpful if EIOPA could also provide the shocks in financial terms. A flexible approach, whereby participants could rely on their internal estimates or, if not possible or practicable, refer to EIOPA's suggested estimates, would be best here. Clear definitions needed for certain metrics (e.g., when do you consider full return to BAU or is processes running again sufficient?). This should be measured against RTO's and RPO's as defined in the BCP's of the entity. Only when you exceed them it is considered as a problem.	
METAMETRIS	Consulting	Cyber resilience shocks can only be defined in technical terms and then be transformed into monetary amounts by each individual entity.	
Cowbell Cyber	Industry	Financial costs should not be prescribed but their calculation basis should be included within the submission.	
IfoA	Association	Financial costs should not be prescribed but their calculation basis should be included within the submission.	
Cyber Resilience: Shocks, Specifications and Metrics	**Type**	**What is your view on the proposed metrics in terms of completeness and viability? Please provide clarification.**	**Response**
Insurance Europe	Association	The proposed metrics are deemed to be sufficient for the most part, as they are aligned with DORA. However, the following slight changes should be made: •Operational Metric: It is stated that "time elapsed until return to business as usual (time to BAU)". This is longer than the duration of the attack itself. Therefore, the industry proposes to use "time of outage or unavailability". •Financial metrics: The statement "loss of revenue corresponding to lost business during the downtime" can only be speculative. This is not considered to be a reliable input and is generally excluded by the operational risk calculation baseline framework since there may be a high level of arbitrariness (eg estimate of customers simply delaying the purchase). The metrics mentioned that are determined to be the most appropriate and complete: •Recovery time •Operational cost •Change in assets and liability •Solvency Capital Requirement •Solvency II ratio	EIOPA takes note of the broad agreement with the metrics proposed and of their higlighted limitations. In particular, with regards to the comments on the usefulness and feasibility of the metric "time elapsed until return to business as usual" and of the inclusion of loss of revenue corresponding to lost business during downtime within "operational and other costs", EIOPA will keep the metrics unchanged as these are seen as essential to assess the impact of the event on the participants' operations and financial position.
GDV	Association	Seems plausible.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry	Table 17 - Cyber resilience metrics: Operational Metric: "Time elapsed until return to business as usual (time to BAU)": this is longer than the duration of the attack itself. We rather support using "time of outage or unavailability". Financial metrics: "loss of revenue corresponding to lost business during the downtime" can only be speculative. We do not consider this to be a reliable input. As an overarching comment, alignment with DORA is important.	
METAMETRIS	Consulting	Metrics have to be complemented for impact estimation see Q25	
Cowbell Cyber	Industry	Complete. However, some elements may need to be defined eg what is sensitive data for the data breach.	
IfoA	Association	Complete. However, some elements may need to be defined e.g. what is sensitive data for the data breach.	
Cyber Resilience: Shocks, Specifications and Metrics	**Type**	**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.**	**Response**
Insurance Europe	Association	The impacts of cyber resilience shocks at the level of business processes identified for all the scenarios seem to be sufficient. It is noted that these impacts need to be major to constitute a resilience shock, with an assessment of the impact performed to link the events to the asset group, also taking into account which application is critical. It must be stated that this question cannot be answered in detail without knowledge of the specifics of the stress scenarios (which scenario, methodology). In addition, a more granular assessment at IT systems level is not supported.	EIOPA takes note of the responses received. While understanding that a more granular assessment of the impact of the shocks at the level of IT systems can in some instances be more precise, at this stage it is considered that a more high-level assessment based on the list of business processes affected is more appropriate as IT-systems are institution-specific and can vary greatly from company to company.
GDV	Association	This cannot be answered without knowledge of the specifics of the stress scenarios (which scenario, methodology).	
AAE	Association	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.	

Institut des actuarires (FR)	Association	The scenarios should be defined at group level and the impact study done at the level of each entity and business line.	
CRO Forum	Industry	We do not support a more granular assessment at "IT systems level". Even the highest level is hard to be quantified. No more granular approach requested. Business processes approach is fine, but requires a better distinction on criticality and potentially guidance from EIOPA.	
METAMETRIS	Consulting	The impact of cyber resilience scenario should be defined at entity and / or business line level.	
Cowbell Cyber	Industry	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.	
IfoA	Association	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.	
Cyber Resilience: Shocks, Specifications and Metrics	**Type**	**What is your view on the exclusion of ransom payments in the context of the ransomware scenario? Please provide clarification.**	**Response**
Insurance Europe	Association	Including ransom payments in the context of the ransomware scenario could be an option as it would give more information on the financial impact. However, it should be excluded in this document as the inclusion could be seen as promoting ransom payments. This can be excluded as the financial impact would not be relevant to factor into "shock metrics" and the legal implications/discussions are not relevant in this scenario. In addition, the payment estimate of ransoms is hardly linkable to the cyber event, since it can be seen as an exogenous variable that does not depend on the magnitude of the cyberattack in any way. For this reason, it could be difficult and off-topic to assess a proper ransom distribution and related statistics.	EIOPA takes note of the agreement to exclude ransom payments from the cyber resilience assessment and this exclusion will be kept in the paper.
GDV	Association	Ok, but could be included as an option.	
AAE	Association	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.	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry	For the purpose of this stress test, the exclusion is reasonable. In practise, there are good reasons why ransoms should not be covered or should be covered in the contracts. There is a clear demand for covering the direct financial consequences of ransomware attacks, such as financial losses resulting from business interruption, the cost for incident response measures but also ransom payment where legally permitted and where they do not fall under any sanction regime. Unfortunately, regulation is very inconsistent across countries. More consistent guidance from regulators and governments would be beneficial for all parties involved. It has a direct financial cost so we assume this could be covered somewhere. It depends on the fact if ransomware payments will/should/could be insured (underwriting part) or if there is an appetite (and it is legal) to pay it (resilience part).	
METAMETRIS	Consulting	Ransom payments may be considered as a lot of companies, including the most mature ones in terms of cyber security, have failed data restauration and testing processes and could have to pay a ransom to recover their data. But if a ransom is paid business disruption shouldn't take place as attackers would be supposed to provide the encryption keys (even though there may be exceptions). Therefore, ransom payment could be excluded to focus on the assessment of the potential damage resulting from business disruption.	
Cowbell Cyber	Industry	This may be appropriate given that the payment of ransoms should not be encouraged as it fuels further bad actor activity.	
IfoA	Association	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.	
Cyber Resilience: Shocks, Specifications and Metrics	**Type**	**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.**	**Response**
Insurance Europe	Association	The identified sources for the calibration of the shocks should be considered as examples only. They should be maintained on an intranet page of EIOPA rather than be recorded in a document, as the sources may change, or newer examples will become available.	EIOPA takes note of the responses received. The sources mentioned in the discussion paper are only examples and should not be seen as exhaustive. In any future stress test exercise on cyber risk, the calibration of the shocks will be made with due caution. To avoid confusion, the references will not be included in the methodological paper.
GDV	Association	No additional suggestions	
AAE	Association	Tesco Bank case study, see answer to Q. 17	
Institut des actuarires (FR)	Association	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.	
CRO Forum	Industry	We believe these sources should be considered as examples only for the moment as this remains a difficult exercise until there is more consistency (through best practice or regulations) on reporting these types of breaches in a structured manner to build historical data. They should be maintained on an intranet page of EIOPA rather than recorded in a document given the sources may move or newer examples will become available.	
METAMETRIS	Consulting	Additional data sources may include: Verizon Data Breach Investigations Report https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/	
Cowbell Cyber	Industry	Fine as a starting point. I cannot think of a comprehensive source so these will have to be considered and interpreted.	
IfoA	Association	Fine as a starting point. We cannot think of a comprehensive source so these will have to be considered and interpreted.	
Cyber Resilience: Shocks, Specifications and Metrics	**Type**	**What is your view on the data collection? Is there any relevant information missing? Please provide clarification.**	**Response**

Insurance Europe	Association	It is just noted that data collection creates an increase in cybersecurity breach risk. As a lower risk approach, the data collected should only be provided to supervisors and only shared on request via secured channels. In relation to the communication of results, the industry would like to highlight the fact that the publication of the results of a cyber stress testing exercise should be approached with extreme caution. In that context, the industry would like to reiterate its position that individual publication is neither necessary nor appropriate for any stress testing exercise. Especially in the context of a cyber stress test, the disclosure of the cyber results, even if these are at an aggregate level, could expose participating undertakings to a great extent by uncovering undertakings' vulnerabilities which can be exploited by malicious parties.	EIOPA takes note of the responses received. Any future data collection will be made with caution through a secured channel. As already stated in chapter 8 of the paper, the process for communicating and disclosing results of a cyber resilience stress test shall be considered with due care and might be adapted to ensure identified vulnerabilities will not be explored by malicious actors.
GDV	Association		
AAE	Association	Tesco Bank case study, see answer to Q. 17	
Institut des actuarires (FR)	Association	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	
CRO Forum	Industry	Data collection creates an increase cyber security breach risk. It would be preferred (e.g. lower risk approach) if overall results only are provided to supervisors and detailed elements are shared on request via secured channels. As mentioned in previous questions clarification should be provided for criticality of business processed and clear definitions (e.g., return to BAU, data breach, sensitive data …). Overall, with the Solvency II framework already providing a stress test on a comparable basis for insurers, there is no need and even strong arguments against publishing the results of EIOPA stress tests that by the very design do not provide comparable results as they are a function of the specific scenario that EIOPA chooses.	
METAMETRIS	Consulting	To limit the data collection effort and ensure some homogeneity across the various insurance groups or entities, a significant number of parameters could be calibrated globally at industry level based on some common assumptions. For example, the duration of business disruption in a worst-case situation (i.e. ransomware attack with active directory compromise) could be defined globally depending on the level of maturity of cyber security within one organization. In the same way the worst-case cost of a data breach per personal data subject (including litigation costs, regulatory fees etc.) could be calibrated for all companies in a given country. In terms of metrics the number of headcounts of the impacted perimeter and new business and attrition indicators may give information on the potential business impacts. Reputation impact depends of the existing attrition rate. If the attrition rate is high, business is sensitive to reputation impact.	
Cowbell Cyber	Industry	Useful to record all the qualitative information listed in addition to the quantitative.	
IfoA	Association	Useful to record all the qualitative information listed in addition to the quantitative.	
General	**Type**	**Remarks**	**Response**
Insurance Europe	Association		Noted.
GDV	Association		
AAE	Association	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.	
Institut des actuarires (FR)	Association		

CRO Forum	Industry	General comments on the whole CP: As always, the CRO/CFO forum suggests EIOPA to adopt a focused, proportionate and practicable approach to its Stress Test exercises. We see EIOPA has reflected this in various areas of the paper such as with Reactive Management Actions or calculation of the post-stress SCR. Indeed, when assessing cyber risks specifically, these have no added value, would only distract from the core of the exercise and increase the operational burden. We also agree with EIOPA's observation that specifically the resilience part is different from the other Stress Tests EIOPA has conducted in the past. Therefore, the application of the proportionality principle would indicate the following: • Scope: the implementation of the stress test should be made at the level where the IT system's security and the cyber underwriting risks are managed. For some groups, this would mean an implementation at group level due to a centralized set-up, but for other groups that are organized more decentralized it would mean an application at solo level. Therefore, the stress test should be built upon a hybrid approach whereby each participant could decide to apply the scenarios at the most appropriate level, following the precedent of the liquidity stress tests. • Metrics: as for financial stress tests, the ultimate financial impact should be depicted through a variation of net asset value. It would be disproportionate to require impacts on P&L, as stress test exercises are macroprudential tools to survey financial stability risks, not the risks for the shareholders. A re-calculation of the SCR should not be required either, as stress tests should not duplicate micro-supervision and not second-guess solvency ratios. • Reactive management actions: while we agree with EIOPA that during real-world event, insurers may resort to a range of management actions to absorb the impacts of a cyber incidents, the "what-if" nature of stress tests does not allow for a meaningful and decision-useful assessment of reactive management actions. Allowing for them would therefore be disproportionate, and would be redundant with other risk management and supervisory tools (ORSA, recovery planning) which are specifically designed for this type of consideration. Reporting: in parts the granularity of the templates does not seem feasible for all our members and as such this needs further consideration. For example, a split by "guarantee" in terms of cost component is not always available and also a split into IT service providers as per table 9.4.3 will not be feasible. Also, some granular data (e.g. exclusions, detailed lines of business, cloud providers) may not be feasible. Therefore, data requirements should focus on indicators that are usually monitored by a typical (re)insurance company. Regarding the cyber resilience part, we would note the developments around DORA, which raises concerns on any discrepancies or actual need for additional cyber testing. It is important for a meaningful and practical implementation of the cyber underwriting exercise that EIOPA takes due consideration of the differences in terms of business and access to data between direct insurers and reinsurers when designing the scenarios, shocks, metrics, and reporting templates. This applies to both affirmative and non-affirmative coverages. Finally, through these exercises EIOPA will collect sensitive individual company data on the cyber security set up of EU insurers that would participate to cyber stress tests. It is key that EIOPA can provide participants assurances that every step will be taken to protect the confidentiality and security of the submissions and data therein.	
METAMETRIS	Consulting		
Cowbell Cyber	Industry		
IfoA	Association		