Questions for Consultation on Issues Paper on Insurance Sector Operational Resilience

Thank you for your interest in the public consultation on the Issues Paper on Insurance Sector Operational Resilience. The Consultation Tool is available on the IAIS website.

Please do not submit this document to the IAIS. All responses to the Consultation Document must be made via the Consultation Tool to enable those responses to be considered.

Consultation questions

1	General comments on the Issues Paper The paper introduces new terms that may not be familiar to some readers. Suggest adding a glossary to the beginning of the paper. “Business Continuity Management” (BCM) is a concept mentioned throughout the paper and in some places, “Business Continuity Planning” (BCP) is used as an interchangeable term. Suggest defining these two terms in a glossary and also clarifying in the paper (see comments for paragraphs 35 and 80) the difference between the two. Presumably BCM encompasses BCP. There are numerous inconsistencies in the use of the Oxford comma (a.k.a. serial comma) throughout the document. For example, paragraphs 25 and 29 omit it, while paragraphs 2 and 24 employ it.
2	General comments on Section 1 Introduction
3	General comments on Section 1.1 Objectives and Scope
4	Comment on Paragraph 1 In the second bullet, add “IT” before “Third-party outsourcing” as this is way the topic is framed throughout the paper and especially in the heading for Section 3.4
5	Comment on Paragraph 2
6	Comment on Paragraph 3 Suggest the following edit to this paragraph. Based on the preceding text, the area of expertise of the stakeholders is implied. The information in this paper is informed by a review of the IAIS Insurance Core Principles (ICPs), a stocktake of existing publications by Standard Setting Bodies (SSBs) with relevance to operational resilience, direct engagement – including roundtables – held with ~~operational resilience~~ experts external to the IAIS membership, and information shared on supervisory practices among insurance supervisors.
7	General comments on Section 1.2 Relevance of operational resilience to the insurance sector
8	Comment on Paragraph 4 Suggest the following edit to the second sentence to improve flow: ~~Thus, t~~The concept of operational resilience is not new, though recognition of the importance of adapting supervisory regimes to account for the growing reliance by insurers on digital systems is more recent.

9	Comment on Paragraph 5 It might strengthen this paragraph to have similar statistics on cyber-attacks between 2019 and 2020, if available, to give some pre-pandemic context. Also, this paragraph is a bit disjointed; there is a number in February and a number in late April, but then goes to the percent increase in May and June compared to March and April. Since the number for March isn't given anywhere, it is hard to know what kind of increase it is over March. For consistency with the use of percent signs elsewhere within the document, suggest replacing "per cent" with a percent sign. Replace "cyber attacks" with "cyber-attacks" for consistency with the other eight occurrences of this word throughout the document.
10	Comment on Paragraph 6
11	Comment on Paragraph 7
12	Comment on Paragraph 8
13	Comment on Paragraph 9
14	Comment on Paragraph 10
15	Comment on Paragraph 11
16	General comments on Section 1.3 Issues Paper structure
17	Comment on Paragraph 12
18	Comment on Paragraph 13
19	Comment on Paragraph 14 Replace both occurrences of "cyber attacks" with "cyber-attacks" for consistency with the other eight occurrences of this word throughout the document.
20	Comment on Paragraph 15 Suggest the following edit to the first sentence to improve flow: The risks posed ~~to insurers~~ by a third-party outsourcing partner for IT-related functions are similar across many industries, including the insurance industry. In this paragraph, consider adding a bit more context around "concentration risk" as the concept is being introduced here.
21	Comment on Paragraph 16 Suggest the following edit to the last sentence; removing "business continuity" eliminates a redundancy and also broadens this statement a bit.

	However, a critical piece of moving to hybrid and remote work environments is understanding and proactively managing the ~~business continuity~~ risks that arise from an increased attack surface, and reliance on technology and outsourcing of critical IT services.
22	Comment on Paragraph 17
23	General comments on Section 2 Applicability of ICPs to operational resilience
24	Comment on Paragraph 18
25	Comment on Paragraph 19
26	Comment on Paragraph 20 Suggest the following edit to the second sentence; modifier not needed. "All of which promote ~~sound~~ operational risk management more generally, while respecting issues of proportionality."
27	Comment on Paragraph 21 The ICPs typically use "sound" in referring to an insurer's management, governance, etc., but not when describing supervision. The ICPs identified as supporting the ~~sound~~ supervision and sound management of operational resilience in the insurance sector include:
28	Comment on Paragraph 22 Similar to paragraph 20, the modifier is not really needed here. The ICPs have clear interactions with operational resilience and support the ~~sound~~ management of an insurer's operational risks.
29	Comment on Paragraph 23
30	Comment on Paragraph 24 Similar to paragraph 21, delete the modifier in this context. The review of ICPs also revealed a number of examples of areas where further discussions or considerations for developing supporting materials could advance the ~~sound~~ supervision of cyber resilience, IT third-party outsourcing, and BCM as critical elements of operational risk management (which are considered among those elements outlined in section 4).
31	General comments on Section 3 Key issues and supervisory approaches
32	Comment on Paragraph 25

33	Comment on Paragraph 26
34	Comment on Paragraph 27 Suggest the following edit to the last sentence to improve clarity: This is particularly important for insurers, in respect of any confidential or personal customer data that is shared with third-party service providers. Inclusion of the word “legacy” in the second sentence implies that all on-premises IT infrastructure is ipso facto obsolete, unable to be updated, nonconforming to security standards, inherently vulnerable, unsupported, unscalable, etc. This simply should not be presumed. The use of advancing technologies could provide cyber security benefit as compared to in-house technology infrastructure and systems, whether legacy or not. The use of advancing technologies, such as the cloud, could provide efficiencies and improvements in cyber security as compared to ~~in-house legacy~~ on-premises technology infrastructure and systems.
35	Comment on Paragraph 28
36	Comment on Paragraph 29 See general comments above and for paragraph 80 – BCP is introduced here without explaining its relationship to BCM. It is also used somewhat interchangeably with BCM. Recommend adding a sentence clarifying the difference between BCM and BCP in this paragraph.
37	General comments on Section 3.1 Governance and Board accountability
38	Comment on Paragraph 30
39	Comment on Paragraph 31
40	Comment on Paragraph 32 The document mentions sound operational resilience, sound practices, sound operational risk management, sound governance, sound management, sound supervision etc., but the word appears misplaced in the following sentence. It should be moved as follows. Recognising that operational disruptions can have widespread impacts across an organisation, the provision of appropriate training across relevant groups within an organisation could facilitate the ~~sound~~ implementation of ~~an~~ a sound operational resilience framework.
41	Comment on Paragraph 33 Suggest the following edit to the first sentence to eliminate redundancy:

	The absence of a framework for identifying – and analysing the impact of – severe but plausible short, medium and long-term risks ~~to operational resilience~~ can limit the chances of successfully enhancing the insurer's overall operational resilience.
42	Comment on Paragraph 34
43	General Comments on Section 3.1.1 Lessons learnt from the pandemic
44	Comment on Paragraph 35
45	Comment on Paragraph 36
46	General comments on 3.1.2 Supervisory approaches
47	Comment on Paragraph 37 Replace "oversight over" with "oversight of" in the first sentence to eliminate the nearly redundant alliteration. Many supervisory authorities currently seek assurance that insurers have sound governance frameworks and adequate Board and Senior Management oversight ~~over~~ of resilience measures, as well as strategies to mitigate risks associated with operational disruption. Additionally, just having and documenting processes isn't enough, so recommend adding a bullet regarding the importance of regularly reviewing/updating processes.
48	General Comments on Section 3.2 Information collection and sharing among supervisors, public/private collaboration Recommend shortening this section name for clarity and consistency with other section titles: **3.2 Information collection and sharing ~~among supervisors, public/private collaboration~~**
49	Comment on Paragraph 38
50	Comment on Paragraph 39 Regarding supervisor and insurer engagement, it seems that in most cases the appropriate engagement is between the supervisor and insurer management (not the board), though the board of course should have a clear understanding of the insurer's operational resilience framework (this is mentioned elsewhere in the paper). To gather this information, some supervisors proactively engage with an entity's ~~Board and~~ Senior Management to understand the effectiveness of an entity's operational resilience framework.

51	Comment on Paragraph 40 Last sentence, beginning and end quotes should be consistent: As the International Monetary Fund (IMF) has noted “[a]ttackers show a degree of agility in cooperation across borders that authorities find difficult to match.’”[11]
52	General comment on Section 3.2.1 Lessons learnt from the pandemic
53	Comment on Paragraph 41
54	General comments on Section 3.2.2 Supervisory approaches
55	Comment on Paragraph 42
56	Comment on Paragraph 43
57	Comment on Paragraph 44 The seventh bullet point references operational *resiliency*, rather than operational *resilience*, which appears 79 times throughout the document. Reports on training delivered in relation to operational ~~resiliency~~ resilience best practices, and in particular on expectations, and roles and responsibilities during periods of sub-optimal functioning;
58	Comment on Paragraph 45 Consider adding “consumer” to the second bullet point as follows: Concerns on data protection and consumer privacy laws that limit or prevent the sharing of information beyond an entity or jurisdiction Further, consider adding an additional bullet as an additional barrier: • Hesitancy of insurer to share information with supervisor because of concerns the information could be used against them, could lead to additional scrutiny of their controls, or that doing so could cause legal risks;
59	General Comments on Section 3.3 Cyber resilience
60	Comment on Paragraph 46 We may be further away from the pandemic once this paper is published, so recommend deleting “has” in the first sentence. Also in the first sentence, there should be a comma after “technologies” to separate the two independent clauses. The insurance sector is heavily dependent on the use of digital technologies, and this reliance ~~has~~ only accelerated during the pandemic as entities transitioned to remote working.

61	Comment on Paragraph 47
62	Comment on Paragraph 48
63	Comment on Paragraph 49
64	Comment on Paragraph 50
65	Comment on Paragraph 51
66	Comment on Paragraph 52
67	Comment on Paragraph 53
68	Comment on Paragraph 54 For this paragraph and heading, it might be more appropriate to refer to “consistent approach” rather than “standardized metrics” to be less prescriptive. The use of “consistent approach” is also more outcomes focused. ***Lack of ~~standardised metrics~~ consistent approach*** Having a consistent~~/standardised~~ approach to assess insurers’ cyber resilience can be helpful especially when insurers are engaging third-party service providers that operate cross jurisdiction (eg cloud).
69	Comment on Paragraph 55 Punctuation is inconsistent. An en dash follows Availability in the first bullet point, while a simple hyphen follows RTO and RPO in the second and third bullet points. All should be en dash characters to maintain consistency with the remainder of the document. Recovery Time Objective (RTO) – defined by the entity… Recovery Point Objective (RPO) – defined by the entity…
70	Comment on Paragraph 56
71	Comment on Paragraph 57
72	Comment on Paragraph 58 Recommend the following edit to avoid using duplicating word choice: One consequence of skills shortages is that the advancement of supervisory frameworks over cyber resilience may lag behind the ~~advancement~~ growing sophistication of cyber-attacks.
73	General Comments on Section 3.3.1 Lessons learnt from the pandemic

74	Comment on Paragraph 59
75	General Comments on Section 3.3.2 Supervisory approaches
76	Comment on Paragraph 60 First sentence of the “Tabletop Exercises” example: Working with US state and federal supervisors, law enforcement agencies, and other officials, under the auspices of the Treasury Department’s “Hamilton” programme, the National Association of Insurance Commissioners (NAIC) facilitates tabletop exercises with insurers and supervisors to explore cyber incident response and recovery~~ back~~. For consistency of the British English spelling used throughout the document, consider changing “programs” to “programmes” in the second sentence under Tabletop Exercises. This aims to enhance cyber response ~~programs~~ programmes of insurers and supervisors by discussing key methods supporting pre-emptive and/or reactive responses to potential threats.
77	Comment on Paragraph 61 The first bullet point requires two corrections, as follows: Self-assessment Questionnaires – involves ~~entity’s~~ entities performing self-assessments of the quality of their cyber resilience framework, the responses to which provide a snapshot of the ~~entity’s~~ entities’ cyber resilience capabilities and vulnerabilities. Suggest the Vulnerability Assessments bullet point be expanded to indicate that these tools are automated scans that check for exploitable known vulnerabilities and culminate in a report on risk exposure. Suggest changing “Cyber incident reporting” to “Cyber Incident Reporting” for case consistency with other titles throughout the document. Suggest changing “Scenario-Based Testing” to “Scenario-based Testing”, for case consistency with other hyphenated titles throughout the document.
78	Comment on Section 3.4 IT third-party outsourcing Suggest additional clarification in this section regarding what is considered a critical and important IT service. As mentioned in paragraph 68, third-party provider risk goes beyond just those that provide IT services.
79	Comment on Paragraph 62 Comment on Paragraph 62

	The last sentence ends awkwardly with two terms that mean essentially the same thing. Recommend striking some text to remove the redundancy. Additionally, "third party" should be hyphenated because it is used as an adjective rather than a noun. However, an area where both supervisory requirements and financial institutions' risk management processes remain less advanced is the identification and management of concentration risks associated with the provision of critical IT services to firms by third-party ~~and outsourced~~ service providers.
80	Comment on Paragraph 63
81	Comment on Paragraph 64
82	Comment on Paragraph 65
83	Comment on Paragraph 66
84	Comment on Paragraph 67
85	Comment on Paragraph 68 Suggest the following edits: Other examples of third-party services often used by insurers that may present concentration risks include processes for annuities, payroll and benefits administration, investment management, claims processing and resolving customer queries.
86	Comment on Section 3.4.1 Lessons learned from the pandemic
87	Comment on Paragraph 69
88	Comment on Paragraph 70
89	Comment on Paragraph 71 The contractual relationship is not at issue, so suggest identifying the third parties as simply *providers*: This was associated with entities having in place numerous arrangements in the same geographic area, resulting in a dependence on one or a few ~~sub-contractors~~ providers in that area for the delivery of services.
90	Comment on Section 3.4.2 Supervisory approaches
91	Comment on Paragraph 72
92	Comment on Paragraph 73
93	Comment on Paragraph 74
94	Comment on Paragraph 75
95	Comment on Paragraph 76

96	Comment on Paragraph 77
97	General Comments on Section 3.5 Business continuity management
98	Comment on Paragraph 78 Suggest using a different word for the following sentence, as to not limit it to only speed: An operational disruption, ~~slowdown~~ degradation or interruption in the activities of an insurer or any of its service providers could jeopardise its ability to meet its commitments to its insureds and other partners.
99	Comment on Paragraph 79
100	Comment on Paragraph 80 Second sentence, similar to the first comments and comments for paragraph 35, recommend adding some additional context around “BCP” or at least referencing an earlier explanation.
101	Comment on Paragraph 81
102	Comment on Paragraph 82 Second sentence, since the IAIS may follow up on some of these considerations, suggest noting that here: The following aspects of BCM are identified as challenges that could benefit from further analysis by the IAIS and/or cooperation amongst supervisory authorities:
103	Comment on Paragraph 83
104	Comment on Paragraph 84 Suggest adding the parenthetical reference “(BIA)” following “Business Impact Analysis.” Also, suggest the following addition to include an example of another area that could be contemplated in a BCP. For example, the need to consider availability in BCPs could be extended to consider the consequences of loss of confidentiality and integrity of information for important business services when business impact analysis (BIA) and risk assessment are performed (information security / cyber preparedness could be integrated into broader BCP and enterprise risk management [ERM]), or how the insurer would handle the loss of a significant number of employees.
105	Comment on Paragraph 85

	If the BIA parenthetical reference is added to paragraph 84, then suggest changing the last sentence accordingly. Additionally, the last sentence of the paragraph should be singular. Continuity assumptions that proved inadequate during the pandemic have led to a review of the criticality of some existing processes and the adoption of different time frames (eg immediate, short, medium and long term) in many operational continuity strategies, depending on the results of their ~~business impact analysis~~ BIA and the needs and resources of each insurer~~s~~.
106	Comment on Paragraph 86 First and second sentences, recommend the following edits. We can already observe that remote work is more permanent. Also, it should be clarified that any additional expenses for remote work are likely attributed to IT security, as remote work in general is often cheaper for organizations. Although hybrid work arrangements ~~might~~ have become more permanent features, in practice remote working policies may vary significantly. Some institutions may consider arrangements that limit the amount of time staff can work from home to avoid additional expenses on IT security.
107	Comment on Paragraph 87
108	General Comments on Section 3.5.1 Lessons learnt from the pandemic
109	Comment on Paragraph 88 Recommend replacing “cyberattacks” with “cyber-attacks” in the last bullet point for consistency with the other eight occurrences of this word throughout the document. It was often seen that third parties had the capability of offering technology solutions that are more secure, resilient, and flexible than financial institutions’ own existing technology solutions, which sometimes rely on legacy systems. The third bullet point is cumbersome but can possibly be repaired by striking one word. Growing customer expectations in relation to the time to recovery and level of recovery, and in terms of effective communication from insurers – ie when a disruption occurs, progress in recovering, ~~and~~ mitigation measures to ensure they can still get serviced, and notification of when services are restored;
110	Comment on Paragraph 89
111	General Comments on Section 3.5.2 Supervisory approaches
112	Comment on Paragraph 90
113	General Comments on Section 4 Summary of observations and potential future areas of IAIS focus

114	Comment on Paragraph 91
115	Comment on Paragraph 92
116	Comment on Paragraph 93
117	Comment on Paragraph 94
118	Comment on Paragraph 95
119	Comment on Paragraph 96 Revision to the first sentence to address a typo: Based on the observations outlined in section 3.4 4, areas that may benefit from further consideration include: In the fourth bullet point, the last sentence identifies small and medium-sized entities but neither qualifies nor quantifies those terms. Accordingly, recommend modifying as follows to denote all but the largest insurers: However, it is recognised that these are complex and costly tools, in particular for ~~small and medium-sized~~ smaller entities.
120	Comment on Paragraph 97
121	Comment on Paragraph 98 First bullet, suggest edit to reflect that the sector is already integrating BCM into other risk management functions: How the sector is approaching evolutions in BCM best practices, in particular in relation to the need to continue to integrate BCM with other relevant risk management functions to remove silos and ensure that BCM frameworks consider the implications of disruptions stemming from cyber and IT third-party outsourcing risks;
122	Consultation Question 1: Do you have views on the relative priority of the observations set out in section 4? Please indicate your preferred prioritisation and any relevant explanations. In our view, cyber incident reporting and concentration risk (as outlined under "IT third-party outsourcing) are key areas that could benefit from additional IAIS discussion. These are areas require supervisory coordination on jurisdictional and global levels and also have implications beyond the insurance sector.
123	Consultation question 2: Are there additional observations for potential future IAIS focus that you view as important to address with respect to insurance sector operational resilience, and which have not been identified in this Issues Paper? If the third-party provider management discussed in this Issues Paper is strictly related to IT services, additional discussion on third-party vendor management as a whole could be useful. If, for instance, a company's producer suffers a cyber-attack or data

	breach or isn't able to resume business in a timely manner after a disaster, that impacts the company's operations, as well. Also, as touched on in Annex 1, there is very little consideration that has been given to fourth-party risks to date. Another item that was touched on briefly but wasn't mentioned as a potential future area of focus is the need to be able to attract and retain talent with expertise in cybersecurity. Training existing staff is a good response, but there has to be existing staff that is interested and there has to be someone or some way to train them. After the training, there still needs to be a way to retain them. Cybersecurity experts are at a premium and although large insurers have the money to pay them, small and mid-sized companies and regulatory agencies don't have the budget.
124	Consultation Question 3: Do you find value in the IAIS facilitating cross-border information sharing to collect information to facilitate a dialogue on operational resilience exposures and best practices? Would you be willing to participate? We think there is value in this assuming it is folded into an existing IAIS forum, such as the revamped Supervisory Forum. It might also be required for such information sharing that participants are signatories to the MMoU. Depending on the forum, we might be interested in participating.