Resolution of public consultation comments on Draft Application Paper on Operational Resilience Objectives

8-8-24 to 11-10-24

No.	Respondent	Public Y/N	Comment	Resolution of comment
General comments on the Application Paper				
1	Gibraltar Financial Services Commission	Yes	The Gibraltar Financial Services Commission published Guidance Notes on Operational Resilience on 20 March 2024 which provides detailed, practical guidance on how in-scope firms (insurers, banks, systemic investment firms, e-money issuers, payment service providers and large insurance intermediaries) should comply with their obligations under the Financial Services (Operational Resilience) Regulations 2023. The Guidance Notes are accessible via the GFSC website here: https://www.fsc.gi/uploads/Guidance%20Notes/GFSC%20Operational%20Resilience%20Guidance%20Note.pdf Separately, Gibraltar's Financial Services (Operational Resilience) Regulations 2023 were also published by HM Government of Gibraltar and can be found here: https://www.gibraltarlaws.gov.gi/index.php/legislations/financial-services-operational-resilience-regulations-2023-7067	Noted
2	Escode (a part of NCC Group)	Yes	Escode (a part of NCC Group) welcomes the opportunity to respond to the International Association of Insurance Supervisors' (IAIS) consultation and offer our expertise as a global software resilience business. With the insurance sectors' increasing reliance on third party providers, and against a backdrop of a fast-evolving threat landscape, it is essential that sound risk management and improved business continuity is embedded in the financial systems' supply chains. We therefore welcome the IAIS' efforts to assess the full range of risks arising from operational risks and promote appropriate and proportionate risk management strategies. With financial authorities globally developing and implementing new frameworks and rules to ensure that these risks are mitigated against, we are hopeful that the IAIS's objectives and toolkit will promote consistency across borders and ensures the full lifecycle of third-party relationships is considered. That said, there are a number of technical changes that would enhance the IAIS's toolkit, ensuring that the full range of risks and (proven) mitigations associated with third-party risk management are reflected. We explore these in the later questions, but at a high-level these cover: • Ensuing that the full-suite of non-technical supply chain risks are embedded in the toolkit, including insolvency, administration and liquidation, transfer of ownership, service deterioration and concentration risk • Requiring the development of "stressed" exit strategies • Bringing the toolkit in line with global regulators' promotion of practical back-up solutions such as escrow We would welcome the opportunity to engage in more proactive dialogue with the IAIS to support your objectives. Indeed, we have positively contributed to other regulatory authorities' consideration of cyber security, operational resilience and third-party risk management, and are eager to do the same with the IAIS.	Noted - to be considered in the development of the Toolkit

No.	Respondent	Public Y/N	Comment	Resolution of comment
			About Escode (a part of NCC Group) With over 30 years' experience protecting business critical software, data and information through escrow, secure verification testing, and cloud hosted software continuity services, as well as significant experience securing digital transformation programs, increasing resilience and reducing risk. NCC Group has followed regulatory developments regarding supply chain risks and third-party arrangements closely, not least to ensure that we, too, are able to meet our customers' evolving demands as regulatory requirements change. We work with customers operating across critical infrastructure sectors who understand how cybersecurity and software resilience can add value and represent a competitive advantage both in their own business as well as across their portfolios. We hold a unique position where we see compliance from the end-user's perspective as well as from the viewpoint of the IT provider and try to assist both in achieving their aims. NCC Group is a global business headquartered in the UK. Through its $220m acquisition of Iron Mountain's Intellectual Property Management division (IPM), has an established and significant footprint in North America, alongside our existing presence in Europe, the Middle East and Asia Pacific. This means we are able to take an international perspective to regulatory approaches to cybersecurity and third-party risk management. The IPM business has been operating in the North America regulatory market for over 30 years. We believe strongly in the potential of appropriate regulatory measures to unleash the innovative ingenuity of adjacent services sectors to develop practical solutions that allow organizations to meet regulatory requirements in the most effective way.	

3	Institute of International Finance	Yes	The Institute of International Finance (IIF) and its insurance members appreciate the opportunity to comment on the IAIS's Draft Application Paper on Operational Resilience Objectives and [Toolkit] (Draft Application Paper or Paper). We share the IAIS's view that, as insurers' operations become more complex, interconnected and dependent on technology and technology-related providers, the likelihood and impact of operational disruptions, and hence, the importance of operational resilience, has increased. The IIF and its members have consistently advocated for a principles-based, outcomes-focused approach to operational resilience that can be interoperable across jurisdictions. The IIF has previously submitted its views in detail on these topics, including in its response to the IAIS's Issues Paper on Insurance Sector Operational Resilience, and in response to the Financial Stability Board's (FSB) consultation, 'Enhancing Third-Party Risk Management and Oversight.' Overarching Comments The Draft Application Paper is an opportunity for the IAIS to advance a common language around operational resilience in the insurance sector through the development of aligned definitions. Aligned definitions for key terms used in the Draft Application Paper, such as critical services, are important in promoting a common supervisory language that promote supervisory coordination and cooperation, particularly for insurance groups with cross-border operations that are subject to both home and host oversight. A common language among insurance supervisors will promote a better understanding of any subsequent recommendations or examples of good practice that may be advanced by IAIS members. Moreover, aligned definitions facilitate the top-down, group-wide approach to operational resilience taken by many insurance groups. This group-wide approach to operational resilience can be undermined and made excessively complex when key definitions and terms do not align. Aligned definitions do not necessarily need to be identical but, rather, conceptually similar definitions. It may be important to reflect market differences in jurisdictional definitions of key terms and this should not be precluded. The IAIS could consider if there is a need for any additional definitions related to operational resilience beyond those contained in the ICPs and ComFrame and include any such definitions in the toolkit as examples that can be elaborated or modified, as necessary, to reflect jurisdictional and market specificities. In the Draft Application Paper, the IAIS should explain how key definitions related to operational resilience are and need to be somewhat different from the definitions employed in other financial services sectors in order to reflect key characteristics of the insurance business model. The IAIS could add considerable value to the cross-sectoral discussions around operational resilience by explaining how concepts developed by other sectoral standard setters and regulators are not necessarily adaptable to the insurance industry given significant differences between the insurance business models and business models in other financial services sectors. Importantly, and as elaborated	Noted – definitions and examples, drawn from supervisory experience, of criteria used to assess the criticality of services to be considered in the development of the Toolkit.

			below, insurers do not provide the critical payment, clearing and settlement services provided by the banking industry, as well as registered clearing agencies and some fintechs. Any final Application Paper should clearly acknowledge that insurers generally do not provide critical services, the disruption of which could cause severe adverse impacts to the global financial system or to the real economy. The Draft Application Paper defines an operationally resilient insurer as one that can encounter, withstand, mitigate, recover and learn from the impact of a broad range of events that have the potential to significantly disrupt the normal course of business by impacting critical services. While we broadly agree with this definition, we note that the insurance sector provides very few critical services and the critical services that some insurers provide generally are less significant and less impactful to customers and to the global financial system or the real economy than those provided by other financial services organizations, particularly banking organizations. While insurers may provide important or mandated insurance products (e.g. auto insurance) or services, these offerings generally are provided by many insurers, allowing for substitutability. In contrast to insurers, the banking sector provides critical payment, clearing and settlement services, the disruption of which could cause severe adverse impacts to the global financial system. Moreover, those services are concentrated in a relatively small number of large global banking organizations, thus creating the potential for systemic risk through the concentration of those services. An insurer should determine whether it any provides critical services in light of the anticipated impact on its customers, the real economy and the global financial system in the event of any substantial disruption of that service. Insurers should be responsible for determining whether they provide critical services, subject to supervisory review and discussion if the supervisor believes that the insurer should characterize a particular service as a critical service. The identification of critical services should not be based on quantitative supervisory thresholds, such as a percentage of market share. Whether a service provided by an insurer is critical should be based on a holistic consideration of the impact on customers, the real economy and the global financial system of a substantial disruption of that service, including the extent to which the disrupted service could be provided by another insurer in an efficient and timely manner. A clear materiality lens should be applied to the determination of whether a service provided by an insurer is a critical service. An overbroad definition of critical services can result in suboptimal operational resilience resource allocation that weakens the overall resilience of the organization. The supervisory approach to third-party (and nth-party) service providers should focus on those service providers that are essential to or support to a material extent the delivery of critical services by an insurer. Similar to the consideration of whether a service provided by an insurer is a critical service, a holistic consideration of the degree of	

			support provided to the insurer by a third- or nth-party service provider is important to determining whether the service provider should be deemed a critical third- or nth-party service provider. This holistic consideration of the degree of support should assess the potential impact of any disruption to the operations of the service provider on the ability of the insurer to continue to provide a critical service to its customers. Insurers should direct their operational resilience resources to those service providers that are essential to or support to a material extent the delivery of a critical service by the insurer. The supervisory approach to third-party (and nth-party) service providers should reflect local rules and local markets. Some supervisors have direct oversight over service providers, while others do not have this authority. The scope of supervisory responsibility and the extent to which responsibility for third-party service providers is vested in other public sector authorities (or shared with other authorities) will influence the operational resilience supervisory framework in a particular jurisdiction. Expectations for insurer oversight of third- and nth-party service providers should reflect local considerations, including market conventions and standard contractual terms. There are also some practical limitations and constraints arising from the market dominance or level of specialization of some vendors. Supervisors may wish to consider the available mechanisms in their jurisdictions that could improve the ability of insurers to obtain appropriate and needed information from their vendors. If the oversight of third-party service providers is not within their supervisory mandates, supervisors could encourage competent authorities to impose customer reporting requirements, consistent with the need to protect a service provider's confidential and proprietary information and data. The IAIS should call on its member supervisors to take a risk-based and principles-based approach to the supervision of operational resilience. The IAIS notes an increase in the importance of operational resilience given the growing complexity of insurance operations and increased interconnectedness. The dynamic nature of operational risk and the need for a nimble response to operational events calls for a principles-based approach to the supervision of operational resilience and the development of a flexible supervisory toolkit that can be applied proportionately to respond to a wide range of operational events with varying levels and scope of impact and materiality. Similarly, insurers should be advised to take a risk-based and flexible approach to operational resilience that recognizes that operational events, their sources and impacts may vary significantly over time and as the activities and operations of the insurer change in response to market developments and opportunities. Overreliance on standardized tools and metrics may overlook emerging threats to sector resilience and may act to constrain insurers' ability to develop new approaches to operational resilience that best suit their activities and unique risk profiles. Insurers should have the flexibility to adopt an operational resilience framework that best reflects their operations, governance and material risks and vulnerabilities. Insurers generally have well established and comprehensive	

			operational resilience frameworks that are integrated into their operations and governance structures. These frameworks encompass risk identification and management, business continuity and crisis management, IT and cyber risk management, and third-party risk management. A Draft Application Paper should reflect examples of good practice and recommendations that have emerged in supervisory discussions among IAIS members. We are concerned that this Draft Application Paper advances new requirements that exceed the scope of the ICPs and the intended scope of an Application Paper. IAIS member supervisors may interpret the language of the Paper as binding recommendations rather than as advice, illustrations, recommendations or examples of good practice that should be applied proportionately and consistent with local rules and practices. We therefore urge the IAIS to ensure that any final Application Paper and the toolkit are designed as a vehicle for sharing insights on emerging best practices and providing insurance supervisors with helpful guidance to support their supervisory oversight activities. We appreciate the language in Paragraph 27 of the Draft Application Paper that emphasizes supervisory communication, collaboration and cooperation, which should be emphasized throughout the Paper. The IIF has engaged in a significant amount of work in the areas of operational risk, operational resilience, cyber risk, and third-party risk management and we would be pleased to share our work as part of this dialogue and as part of related efforts designed to promote operational resilience in the insurance sector. We thank you again for the opportunity to contribute to this consultation and we look forward to the opportunity to provide comments on a draft operational resilience toolkit for the insurance sector. The IIF would be happy to discuss any aspects of this response in more detail.	

No.	Respondent	Public Y/N	Comment	Resolution of comment
4	National Association of Insurance Commissioners (NAIC)	Yes	The terms “supervisor” and “regulator” are used throughout the document. Recommend defining if both terms will be used, or defer to IAIS convention and use “supervisor.”	Agreed - regulator replaced with supervisor.
5	Regulating the independent inspection of insurance and reinsurance claims	Yes	Hello brothers. Of course, I agree with everything contained in the draft and I agree with merging the papers. I hope that there will be two stages after the application on the ground and observing the results of the first stage and evaluating them. So that the second stage will avoid any problems or new developments that may arise in the first stage. Thanks to all the honorable gentlemen who contributed to the preparation and the brothers who participated in the comments.	Noted
6	The Life Insurance Association of Japan	Yes	The Life Insurance Association of Japan (the “LIAJ”) appreciates the opportunity to submit public comments to the International Association of Insurance Supervisors (the “IAIS”) on draft Application Paper (the “AP”) on Operational Resilience Objectives [and toolkit]. The IAIS explains in paragraph 8 that the consultation of the draft Objectives and Toolkit will be conducted separately and will finally be integrated into a single Application paper. As the current consultation only applies to the draft Operational Resilience Objectives, the appropriateness of the Objectives and Toolkit cannot be validated based on a comprehensive assessment. Therefore, the LIAJ may provide additional comments on the Objectives to the upcoming consultation of the draft Toolkit from a combined perspective.	Noted

No.	Respondent	Public Y/N	Comment	Resolution of comment
7	World Federation of Insurance Intermediaries WFII	Yes	General comment WFII appreciates the opportunity offered by the IAIS to comment on the draft Application Paper on Operational Resilience Objectives. WFII and its member associations worldwide welcome and support all guidance given to ensure the resilience of insurance companies. We believe it is important, first and foremost for the protection of policyholders, but also for the public's confidence in the insurance sector and for the stability of the financial system as a whole, that insurers are able to meet the obligations they have entered into at all times. WFII has noted the IAIS' position that its approach to working towards operational resilience of insurers should be dynamic, proportionate, risk-focused, and principles-based. The objectives set out in this Paper reflect this position. What we miss in the Paper, however, is the explicit mention that in many insurance markets around the world all of these objectives are already covered by operational resilience rules. This is certainly the case for the EU with DORA and in the UK with FCA/PRA operational resilience rules. With the publication of this Paper (and in the future the toolkit) there is the potential for it to generate a huge amount of work for firms that have been compliant with the principles for some time. We understand that in some markets the regulatory framework is not as advanced in this regard. We believe the Paper should reflect this and confirm that the UK and EU regimes and potentially other regimes around the world are fit for purpose.	No change - the Objectives do not supersede existing national requirements and it is not the function of an IAIS Application Paper to evaluate whether national regimes are fit for purpose. The toolkit highlights the variety of existing operational resilience practices.
8	General Insurance Association of Japan	Yes	We understand that this application paper does not establish new supervisory objectives, but rather summarizes existing ICP provisions from an operational resilience perspective. As there is no definitive solution to the issue of operational resilience, we ask that the IAIS continue to share the status of its deliberations on this topic with insurers as appropriate. We ask for continued consistency in the development of the draft Toolkit and the drafting of the AP regarding supervisory practices in late 2024.	Noted

9	Google Cloud	Yes	General comments on the Application Paper Google Cloud welcomes the opportunity to provide comments on the IAIS consultative document entitled “IAIS Draft Application Paper on Operational Resilience Objectives [and Toolkit]” (hereinafter “the Consultation”). As the IAIS recognizes, operational resilience is an outcome that should be supported through a wide array of practices, including effective oversight of third-party service providers that impact critical services of insurers. Public cloud technology is one third-party service area becoming increasingly important to insurers. Specifically, insurers are increasingly benefiting from cloud technology in a multitude of ways to understand risk, segment customers, develop new instruments and ultimately offer better and more innovative products to policyholders. Thanks to the cloud, insurers have enhanced capabilities to quickly process large volumes of information, reducing their time to market and providing more agility and scalability at a lower cost. These benefits are fundamental to industry transformation and need to be accounted for in the regulatory guidance. Insurers are choosing to use cloud services because they find the cloud to be equally or more secure and resilient than their existing, often legacy, computing infrastructure. The advancement and competition of cloud technologies in the last few years provide the insurance sector with data protection, data analytics, and operational resiliency capabilities that are more advanced than what individual organizations, especially SMEs and smaller undertakings, can develop on their own. This in turn could lead to greater protection for policyholders and financial stability. At the same time, as adoption has grown, so too have regulatory efforts to understand and address cloud adoption, often resulting in different paradigms and approaches. We believe that clear and enabling principles for insurers to use cloud services are key to regulators’ overall objective to protect policyholders, ensure market integrity, and maintain financial stability. As such, we applaud IAIS's ongoing efforts to enhance operational resilience by setting a defined set of objectives. As a provider of cloud services to the financial services industry, Google Cloud works closely with its financial institution customers to mitigate risks and ensure the seamless provision of cloud services. We believe strongly in supporting the establishment of effective and consistent global regulatory frameworks for such third-party relationships. The Consultation and ongoing work of IAIS are important efforts in this regard.	Noted

No.	Respondent	Public Y/N	Comment	Resolution of comment
10	Global Federation of Insurance Associations (GFIA)	Yes	GFIA appreciates the opportunity to provide its feedback on the IAIS's draft Application Paper on Operational Resilience. Operational resilience is indeed a critical issue for the insurance industry, and GFIA recognises the importance of the work being undertaken in this area. GFIA understands that this application paper does not establish new supervisory objectives, but rather summarises existing ICP provisions from an operational resilience perspective. As there is no definitive solution to the issue of operational resilience, GFIA asks that the IAIS continues to share the status of its deliberations on this topic with insurers as appropriate. GFIA also asks for continued consistency in the development of the draft Toolkit and the drafting of the AP regarding supervisory practices in late 2024. As a general comment, the term "critical" is used across the financial industry in multiple contexts. Consistent guidance on how to apply the word "critical" across multiple risk areas would further support operational resilience programmes.	Noted – definitions and examples, drawn from supervisory experience, of criteria used to assess the criticality of services to be considered in the development of the Toolkit.

11	The Geneva Association	Yes	We appreciate the opportunity to provide our feedback on the IAIS's draft Application Paper on Operational Resilience. Operational resilience is indeed an important issue for our industry, and we recognise the importance of the work being undertaken in this area. We acknowledge the significant work already accomplished by international organisations such as the Financial Stability Board (FSB) and the Organisation for Economic Co-operation and Development (OECD) on operational resilience. It is essential that the IAIS's efforts are aligned and consistent with these ongoing initiatives. We believe that the IAIS should clearly demonstrate how its proposals build on and complement existing international frameworks. In terms of the structure of the paper, we recommend that the "Objectives for insurance supervisors" section be moved to the beginning of section two. Given the IAIS's role as a convenor of insurance supervisors, it should prioritise promoting best supervisory practices. Supervisory guidance is vital to sector-wide operational resilience, and elevating this section would emphasise the importance of coordinated supervisory oversight in preventing conflicting regulatory regimes and providing clearer direction for firms. In section 2.2.3, the introduction of the term "severe operational disruption" may lead to confusion. We suggest either maintaining the widely recognised term "severe but plausible," or providing a clear explanation if the new term is intended to have a different meaning. Consistency in terminology is crucial to avoid ambiguity and ensure clear understanding among stakeholders. In addition, we also suggest that section 2.3.2 be expanded to focus more on interoperability. Promoting the alignment of operational resilience standards across global regulators should be a key objective, and we encourage the IAIS to use its platform to facilitate greater collaboration among regulators on this issue. This would ensure a more consistent and effective global approach to operational resilience. We also wish to highlight the challenges faced in engaging with third-party service providers. In section 2.2.7, while the IAIS encourages insurers to periodically test the Business Continuity Plans (BCPs) of third-party providers, we find that many third parties are often unable or unwilling to share their plans for comprehensive testing. To address this, we recommend that the IAIS suggest alternative methods for assurance, such as seeking validation from third-party providers that their BCPs are regularly reviewed, maintained, and tested. This would provide a reasonable degree of assurance while respecting third-party limitations. Lastly, we seek clarification on the use of the term "critical third-party" in this paper. The term can be interpreted in two distinct ways: • Systemically Critical Third Parties: Entities whose services are essential to the stability of the entire financial sector (as in the UK and EU frameworks).	The IAIS endeavours to collaborate and promote consistency, where relevant, with international standard setting bodies. No change to structure - as all of the content of the Application Paper is applicable to insurance supervisors, the paper is structured such that the objectives aimed solely at insurance supervisors are presented last. Definitions be considered in the development of the Toolkit. Term "severe operational disruption scenarios" changed to "severe but plausible scenarios of operational disruption". Regarding engaging with third-party service providers on testing BCP's, objective 2.7 has been updated to clarify that the insurer should involve critical third-party service providers as needed in the insurer's process to validate that its recovery objectives can be met in a range of severe but plausible scenarios. In this context, consistent with the FSB

			• Firm-Specific Critical Third Parties: Providers whose services are critical to the operations of an individual firm, as understood by the FSB. Clarifying the IAIS's intended definition of "critical third-party" will ensure a consistent understanding and application of the recommendations. We understand that this document forms part of a two-phase consultation, with the second phase, focusing on the toolkit, expected to be launched later this year. While the current phase provides valuable insight into the IAIS's objectives, we believe that a more comprehensive response from our side will be possible once the toolkit has been released. Given the interconnected nature of these two phases, we are of the view that a complete understanding of the IAIS's approach to operational resilience will only be achievable after reviewing the toolkit. Therefore, we anticipate providing more meaningful and substantive feedback at that time. We look forward to the release of the toolkit and the opportunity it will provide to engage more fully with the IAIS on this topic. Thank you for your consideration.	Toolkit for enhancing Third-Party Risk Management and Oversight, the term critical-third party refers to third-parties that provide critical services to the insurer.

No.	Respondent	Public Y/N	Comment	Resolution of comment
12	Central Bank of Ireland	No	I think the Paper is very good in terms of the correct terminology and distinguishing between Risk and Resilience. Our team developed the Central Bank Irelands Cross Industry Guidance on Operational Resilience and developed the Operational Resilience Module for the SSM SREP. The comments made here are to help give more context for firms. We have carried out 3 years of reviews of Insurance Frameworks, particularly high impact insurance firms and some firms do confuse risk and resilience and impact tolerances with RTOs/RPO/Risk Appetite. A key area for firms to fully understand its services is through granular mapping which I feel could be highlighted here more so firms can then find the vulnerabilities in the end to end service.	Agreed – while documenting is intended to encompass mapping, for greater clarity, the term “map” was added to objective 2.1

13	Financial Sector Conduct Authority (South Africa)	Yes	1.1 Background and purpose (4) Consider defining 'operational resilience' 2.1 Relationship amongst operational resilience, governance, and operational risk management This section provides meaningful guidance for the assessment that the supervisors need to consider on the insurer's approach to operational resilience (paragraphs 16 to 18). 2.2.2 The insurer sets impact tolerances for disruption to its critical services (ICPs 8 and 16) (20) Suggested wording: "Defines the maximum acceptable disruption level before it negatively impacts its financial stability, customers, or the broader financial ecosystem." 2.2.4 The insurer effectively manages operational incidents, including but not limited to cyber incidents, affecting critical services (ICP 8) (22) "nth-party service providers," While this may be appropriate for a specialised audience, translating the term into more straightforward language could make the document more accessible. 2.2.7 The insurer develops, implements, tests and updates its BCP and DRP to ensure that it can respond, recover, resume and restore to a pre-defined level of operation following a disruption in a timely manner (ICP 8) (25) Suggested wording: "Creates detailed contingency plans based on defined impact tolerances to mitigate risks to critical services." 2.3.2 Supervisors share information and cooperate with other supervisors with a view to minimising risks (ICPs 3 and 25) (29) Suggested wording: "Defines its strategy for sharing information and collaborating with other supervisors. This strategy should address and minimize legal barriers and other obstacles to cooperation." The bullet points under each objective are informative but can be wordy. Some phrases could be simplified or broken down into more digestible parts for easier comprehension. General comment: Incorporating visual components such as flowcharts or tables might further clarify relationships between objectives, risks, and actions. 2.3.3 Supervisors cooperate and communicate transparently with stakeholders (ICPs 2, 9 and 10) (30) Suggested wording: "Engages with stakeholders including the industry, service providers, government agencies, non-governmental organisations, and policyholders on insurers' operational resilience approaches." 2.3.4 Supervisors support a culture of continuous learning and improvement with respect to operational resilience within the supervisory authority (ICP 2) (31) General comment: Including practical examples or case studies of how these objectives might be applied could also enhance understanding.	Noted - definitions and practical examples to be considered in the development of the Toolkit.

No.	Respondent	Public Y/N	Comment	Resolution of comment
14	Association of British Insurers	No	The ABI welcomes the opportunity to respond to the IAIS Draft Application Paper on operational resilience objectives. We appreciate the work of the IAIS in creating high-level guidance for insurers and supervisors. The ABI agrees that operational resilience globally has gained much needed traction, and many jurisdictions are increasingly looking into appropriate regulatory safeguards. To this end, it is important that approaches to operational resilience are appropriate and reasonably applicable. We welcome the IAIS' definition of operational resilience; this helps ensure greater sector-wide understanding of the concept. However, operational resilience terminology, where possible, should be globally adopted to ensure consistency and sector wide understanding. Furthermore, definitions for key operational resilience terms throughout the IAIS guidance document should also be established. This includes terms such as 'critical service' which appears to be a concept used across jurisdictions but referred to differently. For example, it seems synonymous with the UK's regulatory term 'important business service' and the Canadian term 'critical operation'.	Noted - definitions be considered in the development of the Toolkit.

No.	Respondent	Public Y/N	Comment	Resolution of comment
15	Financial Services Regulatory Authority of Ontario	No	FSRA prudentially oversees Ontario-incorporated insurance companies and reciprocals (“Insurers” or “Sector”). FSRA’s role in the sector includes: 1. Applying a risk based risk-based supervisory framework to identify imprudent or unsafe business practices and misconduct impacting policy holders, customers and subscribers of Insurers and intervene on a timely basis. This framework helps to comprehensively assess the risk profile and determine the overall risk rating of each insurer. 2. Monitoring and regularly reviewing information about an insurer, its industry, and external environment to keep abreast of changes that are occurring or planned in an insurer. Issues include both insurer-specific and sector-wide concerns. 3. Conducting prudential regulation and supervision of Ontario-incorporated insurance companies and reciprocals, including providing regulatory approvals of certain transactions and investments. FSRA's over arching comments are: 1. Would suggest adding that supervisors should look at insurers’ risks from an integrated supervisory perspective, including other related regulated entities under the regulators purview that may impact the insurer. 2. Would suggest integrating assessment of an insurer's operational risk as part of the insurer's overall risk rating. 3. Both of these suggestions would allow for a more comprehensive assessment of an insurer's risks.	Objective 3.2 encourages the sharing of information and cooperating with other supervisors, both within and across jurisdictions. Objective 3.3 emphasises the importance of supervisors integrating expectations for insurance sector operational resilience into its review and reporting frameworks.

No.	Respondent	Public Y/N	Comment	Resolution of comment
16	Liberty, South Africa Insurance Services	Yes	Resilient organisations are those who have nurtured their approaches to the management of risk to the point that they have an organic capacity to respond to, and even capitalise on change, whenever it occurs. Overall, the draft paper is a well-structured and an insightful document that lays a strong foundation for enhancing operational resilience in the insurance sector. The proposed principles are aligned to the Basel Paper on Operational Resilience.	Noted

No.	Respondent	Public Y/N	Comment	Resolution of comment
17	Financial Services Commission Mauritius	Yes	The Financial Services Commission, Mauritius has taken note of the Draft Application Paper on Operational Resilience Objectives [and Toolkit]. IAIS might consider elaborating on the following features as part of the second phase: • Structures including committees and their roles, reporting lines, and establishment of governance bodies and their mandates. • Board engagement, roles and responsibilities: key individual and collective roles of Board, monitoring, reporting and escalation • People and culture: effective governance is underpinned by the people driving resilience initiatives and the fostered culture within firms. Such impact needs to be assessed and incorporated in the framework • Enabling processes and key activities that enable good governance, such as policies, procedures, amongst others. • Industry best practices for operational risk management and business continuity management planning • Climate risk, in particular natural catastrophe which are becoming recurrent (especially for small islands)	Noted – further elaboration on specific aspects of the Objectives to be considered in the development of the Toolkit.
18	Old Mutual South Africa	Yes	Broadly in agreement with the Paper. Explicit emphasis should also be included on premises/facilities, data, (non-tech) third parties and people/teams in addition to the existing strong technology, cyber and 3rd party focus in the existing document. The dependency of insurers on the banking system and (tele)communications infrastructure should also be factored in. Integrated consultation/collaboration between Banks and Insurers should deliver a more resilience Financial Services sector than would be the case without such collaboration. It is also important that operational resilience frameworks are customer-centric and adaptable over time.	Noted
General comments on Section 1: Introduction				
19	General Insurance Association of Japan	Yes	We are aware that the existing APs contain language such as "APs do not set new standards or expectations, but provide supporting material to assist in the implementation of existing standards". We request that it be clearly stated in this AP as well.	This is stated at page 2 of the application paper.
20	Global Federation of Insurance Associations	Yes	GFIA is aware that the existing APs contain language such as "APs do not set new standards or expectations, but provide supporting material to assist in the implementation of existing standards". GFIA requests that it be clearly stated in this AP as well.	This is stated at page 2 of the application paper.

No.	Respondent	Public Y/N	Comment	Resolution of comment
	(GFIA)			
21	The Geneva Association	Yes	We acknowledge the significant work already accomplished by international organisations such as the FSB and the OECD on operational resilience. It is essential that the IAIS's efforts are aligned and consistent with these ongoing initiatives. We believe that the IAIS should clearly demonstrate how its proposals build on and complement existing international frameworks.	Please see the IAIS Issues Paper on Insurance Sector Operational Resilience [link], which includes the outcomes of a stocktake of existing standard setting bodies publications relevant to operational resilience.
General comments on Section 1.1 Background and purpose				
22	Global Federation of Insurance Associations (GFIA)	Yes	To better support consistency across supervisory authorities, the definition should align with existing regulators' definitions. For example, the Canadian federal regulator OSFI's E-21 Guideline defines operational resilience as the "response of a financial institution and its recovery, by taking a holistic approach that considers all critical operations end to end."	Noted - definitions be considered in the development of the Toolkit.
23	Old Mutual South Africa	Yes	Please consider the explicit inclusion: -of all critical third parties, in addition to tech and cyber dependencies, -other critical dependencies such as premises/facilities (location), people (outsourced staff and other BPOs), partners in the "money value chain" (banking system, asset management administrators, asset managers, stock exchanges, etc), tax authorities, partners supporting customer identity verification, etc.	Noted - examples, drawn from supervisory experience, of criteria used to assess the criticality of services (including third-party services) to be considered in the development of the Toolkit.
Comments on Paragraph 1				
24	Old Mutual South Africa	Yes	As insurers' operations become more complex, interconnected and dependent on technology and technology-related providers, as well as other critical third-party and outsource service providers and external participants in execution of the value chain (eg banking system), the likelihood and impact of operational disruptions, and the importance of operational resilience, has materially increased.	Noted
Comments on Paragraph 2				

No.	Respondent	Public Y/N	Comment	Resolution of comment
25	Liberty, South Africa Insurance Services	Yes	This is crucial for fostering consistency while respecting regional differences. Equally, there have been recent incidents that have showcased how disruptive events, (e.g. The CrowdStrike incident) could have a significant impact despite regional footprint. It is therefore critical to ensure that Operational Resilience is approached holistically. Instead of trying to manage specific scenarios, insurers should create the agility and flexibility to cope with turbulent situations, regardless of its cause. This implies mindsets and behaviours should shift equally as much as capabilities to support operational resilience.	Noted
Comments on Paragraph 3				
Comments on Paragraph 4				
26	National Association of Insurance Commissioners (NAIC)	Yes	Suggest removing references that unnecessarily date the paper: Additionally, cyber resilience is identified as one of the IAIS' key strategic themes under its 2020-2024 Strategic Plan. The IAIS 2025-2029 Strategic Plan also features digital innovation and cyber risks as strategic themes.	Reference included as it provides context for work.
27	Financial Sector Conduct Authority (South Africa)	Yes	Consider defining 'operational resilience'	Noted - definitions to be considered in the development of the Toolkit.
Comments on Paragraph 5				
Comments on Paragraph 6				
28	National Association of Insurance Commissioners (NAIC)	Yes	Recommend the following revision to further explain what the Objectives are: These Objectives, as set out in Section 2, are outcomes-based, do not set out new requirements, but rather are supporting material that provide clarity on the application of existing supervisory materials.	These sections in the application paper have been updated compared to the material published in the consultation on the objectives.
Comments on Paragraph 7				
29	Institute of International Finance	Yes	Paragraph 7 defines an operationally resilient insurer as one that can 'encounter, withstand, mitigate, recover and learn from' disruptive events. We note that existing regulations in some jurisdictions also require insurers to 'anticipate' and 'operate through' disruption as well.	No change – this an example of an existing definition. Definitions to be further considered in the development of the Toolkit.

No.	Respondent	Public Y/N	Comment	Resolution of comment
30	National Association of Insurance Commissioners (NAIC)	Yes	As this is a pretty significant summary/definition of operational resilience, recommend setting out in bold font. An operationally resilient insurer is one that can encounter, withstand, mitigate, recover and learn from the impact of a broad range of events that have the potential to significantly disrupt the normal course of business by impacting critical services. Operational resilience takes as a premise the assumption that disruptions will occur and thus that insurers should consider their tolerance for such disruptions and take this tolerance into account when devising their approach to operational resilience.	This is now in the executive summary.
31	General Insurance Association of Japan	Yes	As the term "operational resilience" is used extensively in various parts, it should be redefined (or reposted) and clarified in this AP.	The application paper does not include a section on definitions.
32	Global Federation of Insurance Associations (GFIA)	Yes	As the term "operational resilience" is used extensively in various parts, it should be redefined (or reposted) and clarified in this AP.	The application paper does not include a section on definitions.
33	Financial Sector Conduct Authority (South Africa)	Yes	The next sentence explains operational resilience as an outcome and in broader context. Perhaps adding the definition right at the beginning will tie it nicely with the outcome.	The application paper does not include a section on definitions.
34	Liberty, South Africa Insurance Services	Yes	Anticipate, Adapt and Evolve should be considered as part of the definition. Operational disruptions could also be initiated through necessary change/disruption, which requires insurers to take urgent action to ensure its relevance and uphold competitive advantage.	The application paper does not include a section on definitions.
Comments on Paragraph 8				
35	National Association of Insurance Commissioners (NAIC)	Yes	Section 3 as the Toolkit placeholder describes the two phases of this project, for purposes of the consultation. Suggest deleting this paragraph and revisit including such a description as part of the single Application Paper.	These sections in the application paper have been updated compared to the material published in the consultation on the objectives.

No.	Respondent	Public Y/N	Comment	Resolution of comment
36	The Life Insurance Association of Japan	Yes	The IAIS explains in paragraph 8 that the consultation of the draft Objectives and Toolkit will be conducted separately and will finally be integrated into a single Application paper. As the current consultation only applies to the draft Operational Resilience Objectives, the appropriateness of the Objectives and Toolkit cannot be validated based on a comprehensive assessment. Therefore, the LIAJ may provide additional comments on the Objectives to the upcoming consultation of the draft Toolkit from a combined perspective.	Noted
37	General Insurance Association of Japan	Yes	We expect that a proportional approach will be adopted in the development of supervisory practices in late 2024, taking into account regional and jurisdictional circumstances, rather than adding new requirements, etc.	Application papers do not set out new requirements and the proportionality principle is applicable throughout.
38	Global Federation of Insurance Associations (GFIA)	Yes	GFIA expects that a proportional approach will be adopted in the development of supervisory practices in late 2024, taking into account regional and jurisdictional circumstances, rather than adding new requirements, etc.	Application papers do not set out new requirements and the proportionality principle is applicable throughout.
39	Central Bank of Ireland	No	The Central Bank of Ireland have a Supervisory Operational Resilience Toolkit developed. This is now widely used by supervisors to assess their firms maturity. It contains an information request for documents from the firm. A question bank on all the different areas of operational resilience from governance through to lesson learned. it allows for a firm to fill out a self assessment area to generate a maturity graph. this can be done for a single firm view and a sector as a whole. It also contains definitions of operational resilience and an area to send us the SMEs an email if they have queries.	Noted - to be considered in the development of the Toolkit.
General comments on Section 1.2 How ICPs support operational resilience				
Comments on Paragraph 9				
Comments on Paragraph 10				
40	National Association of Insurance Commissioners (NAIC)	Yes	To help with readability, suggest: A key aspect of operational resilience is that operational disruptions can have both narrow and wide-spread implications, (for example, to a functional area of the insurer, across the organisation, sector-wide, across sectors and/or across jurisdictions).	Updated and now in section 2.2.
Comments on Paragraph 11				

No.	Respondent	Public Y/N	Comment	Resolution of comment
41	National Association of Insurance Commissioners (NAIC)	Yes	The word choice is a bit odd; suggest: A number of ICPs both individually and when viewed holistically collectively, support the sound supervision... Add a bracket here for consistency: ICP 25 (Supervisory Cooperation and Coordination)	Edits made.
General comments on Section 2: Objectives for insurance sector operational resilience				
42	Google Cloud	Yes	General comments on Section 2 Objectives for insurance sector operational resilience We welcome the IAIS decision to limit the application of the key operational resilience objectives set out in the Consultation to the delivery of critical services. However, as the Consultation does not define “critical services” or provide any conditions which may be used to assess when a service should be considered critical, insurers may be left uncertain and respond by taking steps to implement the objectives for non-critical and lower risk services. This may result in resources being drawn away from genuinely critical services and create practical challenges where requirements are not aimed at or suitable for lower risk arrangements. Setting out clearly defined criticality criteria, or a minimum threshold, will reduce the burden for regulated entities when implementing the objectives. It will also provide more consistency with IAIS’s approach of applying the principle of proportionality to the implementation of the objectives. We therefore request that IAIS consider providing a proportionate set of criteria for assessing when services should be considered critical.	Reference to the definition of critical services set out in the FSB Toolkit for Enhancing Third-Party Risk Management and Oversight added on page 13, footnote 3. Examples, drawn from supervisory experience, of criteria used to assess the criticality of services to be considered in the development of the Toolkit.

No.	Respondent	Public Y/N	Comment	Resolution of comment
43	Association of British Insurers	No	The ABI supports the rationale and basis provided by the IAIS for the operational resilience objectives. We especially acknowledge the interconnected nature of the topic and the importance of sound objectives which help to mitigate against the risks presented to sound operational resilience and to ensure a high degree of resilience.	Noted
44	Old Mutual South Africa	Yes	Although the Operational Resilience principles set out in the following section of the consultation paper are broadly aligned to the Basel Seven Principles of Operational Resilience, it may be simpler to adopt them directly - especially given Insurers' dependency on the banking industry. Principle 1 – Governance Principle 2 – Operational Risk management Principle 3 - Business continuity & Testing Principle 4 – Mapping of Interconnections and Interdependencies of Critical Operations Principle 5 – Third- Party Dependency management Principle 6 – Incident management Principle 7 – Resilient ICT & Cyber Security	No change – The IAIS endeavours to collaborate and promote consistency, where relevant, with international standard setting bodies.
Comments on Paragraph 12				
45	National Association of Insurance Commissioners (NAIC)	Yes	To help with readability, suggest: ...rely on third-party services to support their operations (some of which are critical to the insurer's business viability) and are increasingly subject to operational risks that may be systemic in nature.	Agree
46	Old Mutual South Africa	Yes	Reference to the dependency on banking system and (tele)communication infrastructure should be included here.	No change – as the Objectives are intended as high-level and principles-based explanatory material, dependence on specific industries is not referenced. Examples, drawn from supervisory experience, of criteria used to assess the criticality of third-party services to be considered in the development of the Toolkit.

No.	Respondent	Public Y/N	Comment	Resolution of comment
Comments on Paragraph 13				
Comments on Paragraph 14				
47	National Association of Insurance Commissioners (NAIC)	Yes	Suggest further expanding on what the Objective are and how they are written: The objectives are written as an outcomes-based articulation of the application of existing ICPs; they do not set out new supervisory requirements. The ICP relevant to each Objective is indicated. Each Objective is followed by additional relevant considerations. So it is more clear, consider moving this to a separate paragraph below and renumbering subsequent paragraphs accordingly: While Sections 2.1 and 2.2 are directed at insurers, supervisors would also benefit from considering these outcomes when setting out their supervisory initiatives.	Agree
Comments on Paragraph 15				
General comments on Section 2.1 Relationship amongst operational resilience, governance, and operational risk management				
48	National Association of Insurance Commissioners (NAIC)	Yes	Consider including the ICP topic or hyperlinking back to ICP listing in Section 1 for each linked ICP in the subsections.	Agree
49	Global Federation of Insurance Associations (GFIA)	Yes	The communication requirement is too broad, especially regarding regulation authorities.	Application papers do not set out requirements. Regulatory authorities removed as this is implicit in the reference to key stakeholders.
50	Financial Sector Conduct Authority (South Africa)	Yes	This section provides meaningful guidance for the assessment that the supervisors needs to consider on the insurer's approach to operational resilience (paras 16 to 18)	Noted
Comments on Section 2.1.1				
Comments on Paragraph 16				

No.	Respondent	Public Y/N	Comment	Resolution of comment
51	Global Federation of Insurance Associations (GFIA)	Yes	GFIA supports the objective of board oversight regarding an insurer's engagement in operational resilience. This objective is consistent with the US NAIC Insurance Data Security Model Law, which provides that each board must "require its executive management or delegates to develop, implement, and maintain an information security program. The Model Law also provides that each board must require annual reports detailing risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program." While the emphasis on the role of the board in overseeing operational resilience is appropriate, the paper does not provide sufficient detail on how supervisors will assess the adequacy of board involvement. Insurers need more clarity on the level of reporting and oversight expected, particularly in light of differing governance structures across firms. This section would benefit from more specific guidance on what constitutes effective board engagement in resilience matters, without imposing undue administrative burdens.	Noted - more information is now included in the application paper, together with practices.

No.	Respondent	Public Y/N	Comment	Resolution of comment
52	Association of British Insurers	No	The ABI supports the need for insurers to adequately manage and mitigate the impact of technology-related risks to critical services through implementing an effective approach to operational resilience. In particular, we note and support the need for collaborative approaches. The ABI believes collaboration to mitigate against operational risks should be supported. For instance, in the UK, the Prudential Regulation Authority set up subject expert groups (SEGs) with industry to discuss regulatory proposals in areas such as Solvency UK, stress tests and liquidity risk. The SEGs have proven to be a valuable mechanism for bringing key stakeholders together for dialogue on important topics. This model of engagement could be replicated by IAIS and at national level. Such a group could bring together firms, the Regulators and relevant stakeholders such as third parties to discuss and develop ideas around topics like scenario testing, incident management and self-assessments. Such a forum could also facilitate discussions and sharing of any lessons learned from incidents. Another example of successful collaboration that can be found in the United Kingdom is the Cross Market Operational Resilience Group (CMORG). This initiative, which is co-led by the Bank of England and the financial services industry, is another successful mechanism to discuss and develop operational resilience topics to test and, if appropriate, identify potential enhancements to the existing framework. The group also has various sub-groups, some of which are sector specific such as the Insurance Sector Operational Resilience Group (ISORG), resulting in a useful permanent mechanism to enhance collaboration between regulators and industry and ultimately aimed at yielding tangible, pragmatic and proportionate results.	Noted
53	Liberty, South Africa Insurance Services	Yes	Apart from oversight, inclusive of providing direction and steer, the board and senior management would not manage any other activities related to operational resilience; they will however have to ensure that resources including people capacity, financial or otherwise are allocated, those who have a core responsibility to steer the overall operational resilience capability for the organisation.	Noted

No.	Respondent	Public Y/N	Comment	Resolution of comment
Comments on Paragraph 17				
Comments on Section 2.1.2				
54	National Association of Insurance Commissioners (NAIC)	Yes	Revise to reinforce the Board's ultimate responsibility for ensuring that the insurer has effective systems in place and management effectively implements them. The Board ensures the insurer's approach to operational resilience leverages, and is integrated with, its operational risk management framework in a consistent, comprehensive and robust manner (ICP 8)	More information is now included in the application paper, together with practices.
55	Central Bank of Ireland	No	IAIS should consider including the approach to operational resilience should be done holistically across multiple business lines/functions. Consider the Operations pillars as the leader and the 2nd line to review and approve. All elements of the Framework should be reviewed and approved by the Board. Operational Resilience must be integrated into various committees' Terms of Reference and establish a structured reporting line to the Board. The more mature firms typically have the Chief Operating Officer (COO) spearheading the Framework's implementation.	The three lines of defence are referenced in objective 1.2 and in examples of practices.
Comments on Paragraph 18				
56	National Association of Insurance Commissioners (NAIC)	Yes	Footnotes are being removed from the ICPs for consistency; for the third bullet suggest: (eg the division of responsibilities between the business, risk management and compliance and internal audit, as referred to at ICP 8.2.4 2)	Update made to objective 1.2.
57	The Life Insurance Association of Japan	Yes	As to the second bullet point of paragraph 18 which recommends that insurers' approach to operational resilience "identifies and manages all risks that have the potential to severely disrupt its operations", the appropriateness for requiring insurers to identify and manage all the risks would depend on the potential to severely disrupt operations, and the degree of severity. The LIAJ believes a more adequate review to the appropriateness of this Objective is possible in conjunction with the Toolkit. The current consultation only includes the draft Objectives so it is difficult to conduct a comprehensive assessment without looking at the draft Toolkit. Therefore, the LIAJ may provide additional comments on the Objectives to the upcoming consultation of the draft Toolkit from a combined perspective.	Noted

No.	Respondent	Public Y/N	Comment	Resolution of comment
58	Global Federation of Insurance Associations (GFIA)	Yes	GFIA supports the objective for insurers to have an approach to operational resilience that is consistent, comprehensive and robust. This is consistent with the US NAIC Insurance Data Security Model Law, which provides that each insurer must "design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody, or control." The Model also specifies a number of security measures insurers must consider, requires that cybersecurity risks be included in the enterprise risk management process, calls for insurers to stay informed on emerging threats and vulnerabilities and for personnel to receive cybersecurity awareness training. While the integration of operational resilience with the broader risk management framework is mentioned, the paper does not sufficiently address the complexities that insurers face in operationalising this integration. The paper could benefit from more detailed guidance on how these principles will be applied to insurers of varying sizes and structures. It would be useful to clarify the flexibility supervisors will allow in adapting resilience frameworks to different organisational contexts, avoiding a one-size-fits-all approach.	The application paper now makes a number of references to integration into risk and governance frameworks. Additionally, the proportionality principle set out in the ICPs applies to the application paper.
59	Liberty, South Africa Insurance Services	Yes	Operational resilience and operational risk are interdependent and enhancing resilience directly contributes to better management of operational risks. This point in conjunction with identifying critical services and mapping interdependencies would contribute significantly to effectively managing risk holistically.	Noted
General comments on Section 2.2 Key elements of a sound approach to operational resilience				
60	National Association of Insurance Commissioners (NAIC)	Yes	Consider including the ICP topic or hyperlinking back to ICP listing in Section 1 for each linked ICP in the subsections.	Agree

No.	Respondent	Public Y/N	Comment	Resolution of comment
61	Central Bank of Ireland	No	The above IAIS Guidance on critical services may be too high level for a firm to understand its importance in becoming operationally resilient and how to correctly identify its Critical Services. The Guidance should also outline that companies must establish criteria for determining whether a service is considered critical. Mature firms would have a methodology in place. A firm should leverage its existing business functions' knowledge when identifying and prioritising its critical or important business services. As critical or important business services will differ between individual firms and sectors, firms should take an outcomes based approach to identification of these services.	Reference to the definition of critical services set out in the FSB Toolkit for Enhancing Third-Party Risk Management and Oversight added on page 13, footnote 3. Examples, drawn from supervisory experience, of criteria used to assess the criticality of services have been considered the Toolkit.
62	Old Mutual South Africa	Yes	Outside of this principle-based paper, organisations may benefit from more detailed guidance on service identification and mapping and ensuring completeness of the critical services inventory, as this is where the practical challenges of implementation are experienced.	Examples, drawn from supervisory experience, of criteria used to assess the criticality of services, mapping and developing a critical services inventory to be considered in the Toolkit.
Comments on Section 2.2.1				
53	National Association of Insurance Commissioners (NAIC)	Yes	Revise to reinforce the Board's ultimate responsibility for ensuring that the insurer has effective systems in place and management effectively implements them. The Board ensures the insurer identifies and maintains an up-to-date inventory of its critical services and interdependencies (ICP 8)	The material in the toolkit includes more information on the role that Boards and Senior Management play in different jurisdictions.

No.	Respondent	Public Y/N	Comment	Resolution of comment
64	Global Federation of Insurance Associations (GFIA)	Yes	The language found on page 7, “Identifies and documents each critical service end-to-end and the related interdependencies, including, but not limited to, connections with third- and nth-party service providers,” seems to imply documenting the subcontracting chain as a whole. GFIA suggests limiting it to “material subcontractors” as in the DOR	No change – this Objective emphasises the importance of identifying an insurer’s critical services, and mapping these to the third and nth party service providers that create an interdependency, and hence which are important to the delivery of the critical service.
65	Central Bank of Ireland	No	Firms are carrying out self-assessments on its critical services and presented annually to the board.	Noted
Comments on Paragraph 19				

No.	Respondent	Public Y/N	Comment	Resolution of comment
6	Google Cloud	Yes	Comments on paragraph 19 IAIS has set the objective for insurers to keep an up-to-date inventory of its critical services and their interdependencies including connections with third- and nth-party service providers. Google Cloud recognizes the importance of ensuring visibility over the critical services of insurers, including the parts of those services delivered through service provider supply chains. To promote certainty and focus resources on activities that have the most impact on operational resilience, we suggest clarifying that insurers obtain only information regarding critical third- and nth-party providers and not all third- and nth-party providers which form part of the supply chain for a critical service. Not all third- and nth-party service providers that deliver services as part of the supply chain of an insurer's critical services will form a material part of it or have an impact on operational resilience. Focusing on third and nth- party services that actually have an impact on operational resilience will prevent the over-reporting of information that is immaterial to operational resilience and reduce the undue administrative burden on regulated entities. It will also help supervisors by protecting against diluting the focus away from the information obtained regarding material third and nth-party providers that has a significant impact on operational resilience. We suggest therefore that paragraph 19 bullet 2 be amended to include the word "critical" so that it reads as follows: "Identifies and documents each critical service end-to-end and the related interdependencies, including, but not limited to, connections with CRITICAL third- and nth-party service providers."	No change - this Objective emphasises the importance of identifying an insurer's critical services, and mapping these to the third and nth party service providers that create an interdependency, and hence which are important to the delivery of the critical service.

No.	Respondent	Public Y/N	Comment	Resolution of comment
67	Global Federation of Insurance Associations (GFIA)	Yes	In the first bullet, IAIS is using the term “critical service” which is to be used synonymously with Important Business Service (UK - PRA/FCA), Critical or Important Business Service (Ireland - CBI), or Critical Operations (Canada - OSFI). If there was an opportunity for the IAIS to advise regulatory bodies to align on a singular term it would be welcomed. In the second bullet, the IAIS may want to consider changing ‘nth-party’ to ‘critical nth-party’ when mapping critical services. There would be countless 4th, 5th, nth parties to any third-party arrangement. The current wording is ambiguous as it does not distinguish which nth parties should be documented. It is also unclear how organisations will be able to identify interdependencies/connections with nth-party service providers. Due diligence on an organisation’s critical services provided by third parties should suffice.	Definitions and examples of practices relevant to the identification of interdependencies with nth party service providers to be considered in the development of the Toolkit. No change to use of term “nth party” - this Objective emphasises the importance of identifying an insurer’s critical services, and mapping these to the service providers that create an interdependency, and hence which are important to the delivery of the critical service.
68	Central Bank of Ireland	No	Where its states - Identifies and documents each critical service end-to-end and the related interdependencies, including, but not limited to, connections with third- and nth-party service providers. could the IAIS consider; Mapping is a key element of Operational Resilience, it helps the firm understand all the interdependencies and Interconnections involved in delivery its critical or important business services but more importantly it provides the firms with evidence where the vulnerabilities lie. We have experienced this from our inspections and many firms in the insurance sector are now addressing the vulnerabilities identified during the mapping stage. I think documenting it would fall short of what is required and the benefit from it.	Agreed – mapping is added at objective 2.1.

No.	Respondent	Public Y/N	Comment	Resolution of comment
69	Liberty, South Africa Insurance Services	Yes	Identifying critical services and mapping interdependencies within any organisation and by virtue, its ecosystem is essential for understanding vulnerabilities and enhancing operational resilience and an invaluable piece of work, but it can be quite complex and requires intense commitment. The biggest challenge that insurers are likely to encounter with this is the availability of data and maintaining that data once it is consolidated. However, this has the potential to become a real game changer for managing risk and understanding impact, if done systematically. Consider requesting country regulators/supervisors to provide steer on what critical services should entail to achieve consistency.	Examples, drawn from supervisory experience, of criteria used to assess the criticality of services and mapping interdependencies considered in the Toolkit.
Comments on Section 2.2.2				
70	National Association of Insurance Commissioners (NAIC)	Yes	Revise to reinforce the Board's ultimate responsibility for ensuring that the insurer has effective systems in place and management effectively implements them. The Board ensures the insurer sets impact tolerances for disruption to its critical services (ICPs 8 and 16)	The material in the toolkit includes more information on the role that Boards and Senior Management play in different jurisdictions.

No.	Respondent	Public Y/N	Comment	Resolution of comment
71	Central Bank of Ireland	No	It is good to see the impact tolerance explained as the maximum disruption to a critical service As there is some confusion around this in Industry, maybe greater clarity or expectation of firms is needed; While impact tolerances should be aligned to a firm's risk appetite, impact tolerances are a separate and distinct tolerance measurement. Risk appetite focuses on the impact and probability of a risk event occurring and is typically set with reference to a firm's strategic goals. Impact tolerances assume that the risk event has already crystallised and, therefore, the probability element of risk appetite is removed. When a disruption has impacted a critical or important business service the risk appetite will have already been breached. Impact tolerances are a standard that a firm should be able to remain within and which the board and senior management should use to drive improvements to its operational resilience.	Noted
Comments on Paragraph 20				
72	General Insurance Association of Japan	Yes	Since operational disruption/impact is not always quantifiable, we suggest replacing "Quantifies" in the first bullet point with "Understands" or additionally describing that there are cases where it is impossible to quantify maximum disruption/impact. The second bullet point: Regarding "pre-defined", we would like to clarify this means that each entity defines its own "tolerances".	In objective 2.2 "quantifies" has been changed to"defines". The second bullet is to be read in conjunction with objective 2.2, which refers to the insurer setting its impact tolerance.

No.	Respondent	Public Y/N	Comment	Resolution of comment
73	Global Federation of Insurance Associations (GFIA)	Yes	GFIA supports the objective for insurers to understand the potential damage that a disruption in critical services can cause. This objective is consistent with the US NAIC Insurance Data Security Model Law, which requires each insurer to “assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information.” In the first bullet, quantifying the maximum disruption/impact for each process may be a challenge for some organisations. Both quantitative and qualitative factors should be considered. Since operational disruption/impact is not always quantifiable, "Quantifies" in the first bullet point should either be revised to "Understands", or additionally wording should be included to explain that there are cases where it is impossible to quantify maximum disruption/impact. In the second bullet, regarding "pre-defined", we would like to clarify this means that each entity defines its own "tolerances".	In objective 2.2 “quantifies” has been changed to”defines”.
74	Central Bank of Ireland	No	as above	Noted
75	Financial Sector Conduct Authority (South Africa)	Yes	Suggested wording: "Defines the maximum acceptable disruption level before it negatively impacts its financial stability, customers, or the broader financial ecosystem."	In objective 2.2 “quantifies” has been changed to”defines”.
76	Old Mutual South Africa	Yes	Practical guidance for setting and testing thresholds for non-tech services would be helpful as this is particularly challenging.	Noted – information in the Toolkit.
Comments on Section 2.2.3				
77	National Association of Insurance Commissioners (NAIC)	Yes	Revise to reinforce the Board's ultimate responsibility for ensuring that the insurer has effective systems in place and management effectively implements them. The Board ensures the insurer self-assesses and tests its ability to withstand and recover from severe operational disruption scenarios, and ensures that action is taken to improve operational resilience on the basis of lessons learnt (ICPs 8 and 16)	More information is now included in the application paper, together with practices.

No.	Respondent	Public Y/N	Comment	Resolution of comment
78	General Insurance Association of Japan	Yes	We agree on the importance of scenario testing with severe but plausible scenarios. On the other hand, it is not easy to prepare exhaustive scenarios because there are many possible factors that can affect operational resilience. Scenario testing is only one of various ways to improve operational resilience, and therefore, instead of preparing exhaustive scenarios, only those scenarios that are truly probable and important should be carefully selected for implementation.	Noted – the text refers to severe but plausible scenarios of operational disruption and is not intended to imply the need to prepare exhaustive scenarios.
79	Global Federation of Insurance Associations (GFIA)	Yes	GFIA agrees on the importance of scenario testing with severe but plausible scenarios. On the other hand, it is not easy to prepare exhaustive scenarios because there are many possible factors that can affect operational resilience. Scenario testing is only one of various ways to improve operational resilience, and therefore, instead of preparing exhaustive scenarios, only those scenarios that are truly probable and important should be carefully selected for implementation. The requirement for insurers to perform self-assessments of their resilience to operational disruptions is reasonable, but the paper lacks specific recommendations on how supervisors will ensure that these assessments are appropriately tailored to the operational realities of each insurer. The guidance should recognise that smaller insurers or those with less complex operations may need different approaches compared to larger, more complex entities. A clearer recognition of proportionality would enhance the practical applicability of the self-assessment framework. The introduction of the term “severe operational disruption” may lead to confusion. GFIA suggests either maintaining the widely recognised term “severe but plausible” or providing a clear explanation if the new term is intended to have a different meaning. Consistency in terminology is crucial to avoid ambiguity and ensure clear understanding among stakeholders.	Agreed – “severe operational disruption scenarios” changed to “server but plausible scenarios of operational disruption” in objective 2.3. Examples of practices relevant to these assessments to be considered in the development of the Toolkit.

No.	Respondent	Public Y/N	Comment	Resolution of comment
80	The Geneva Association	Yes	In section 2.2.3, the introduction of the term “severe operational disruption” may lead to confusion. We suggest either maintaining the widely recognised term “severe but plausible,” or providing a clear explanation if the new term is intended to have a different meaning. Consistency in terminology is crucial to avoid ambiguity and ensure clear understanding among stakeholders.	Agreed – “severe operational disruption scenarios” changed to “server but plausible scenarios of operational disruption” in objective 2.3.
81	Central Bank of Ireland	No	IAIS should consider including how vulnerabilities will be addressed as an outcome of the testing. The Scenario testing results should be reviewed and approved by the Board. The purpose of scenario testing should be to test a firm’s ability to remain within its impact tolerances through severe but plausible scenarios.	Objective 2.3 encourages that the insurer “Incorporates lessons learnt from scenario testing, particularly when the results of testing identify that tolerances for disruption would be breached in one or more severe but plausible scenario. More information is now included in the application paper, together with practices.
Comments on Paragraph 21				
82	Global Federation of Insurance Associations (GFIA)	Yes	The IAIS outlines that scenario testing should be embedded to focus on operational resilience and assess the insurer’s ability to withstand and recovery from severe but plausible operational disruptions. This is valid but additional guidance on how this applies specifically to critical services (eg end-to-end testing) would support the role of scenarios in the testing of critical services.	Noted - scenario
83	Central Bank of Ireland	No	Agree - Self-assessments are key as business models change, services change and annual testing to remain within impact tolerances should be carried out	Noted
Comments on Section 2.2.4				

84	Escode (a part of NCC Group)	Yes	We are in favour of a broader definition of supply chain resilience that looks beyond technical risk (e.g. cybersecurity) and takes a wider approach to understanding what is needed to safeguard continuity of service and operational continuity against non-technical risks such as insolvency, administration and liquidation, transfer of ownership, service deterioration, and concentration risk. We have sought to introduce to regulators' considerations of supply chain resilience the concept of 'Resilience by Design', assuming supplier failure by default, and taking a two-fold approach to mitigating the associated risks that include: • prevention of supply chain failure (through cyber resilience solutions); and, • mitigation of the risk and impact of supply chain failure (through technology and software/data escrow agreements). In practice, this includes naming supplier failure, service deterioration and concentration risk as risks that require mitigation strategies (e.g. through stressed exit plans and scenario testing) and assigning ownership for third-party risk at the highest-possible level. This holistic approach has been adopted across several regulators globally, including the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB) , and the Office of the Comptroller of the Currency (OCC) (https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html), as well as the Prudential Regulatory Authority (PRA) in the UK (https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf?la=en&hash=5A029BBC764BCC2C4A5F337D8E177A14574E3343), the European Union (https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/) and the Monetary Authority of Singapore (https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf). We ask that this evolving approach to supply chain resilience is reflected in the IAIS's toolkit, with supplier failure, service deterioration and concentration risk named as operational risks and incidents that need to be understood and mitigated against, in section 2.2.4.	Noted and included in the Toolkit.

No.	Respondent	Public Y/N	Comment	Resolution of comment
85	National Association of Insurance Commissioners (NAIC)	Yes	Revise to reinforce the Board's ultimate responsibility for ensuring that the insurer has effective systems in place and management effectively implements them. The Board ensures the insurer effectively manages operational incidents, including but not limited to cyber incidents, affecting critical services (ICP 8)	More information is now included in the application paper, together with practices.
86	Global Federation of Insurance Associations (GFIA)	Yes	The incident reporting should be limited to major incidents.	The proportionality principle would apply here.
Comments on Paragraph 22				
87	Google Cloud	Yes	Comments on paragraph 22 Google Cloud recognizes the importance for insurers to have clear processes for identifying, reporting and responding to incidents, including where incidents relate to the services they receive from third parties. However, an objective for insurers to have processes for ensuring that its third- and nth-party service providers identify, report and respond to any incident which affects them and impacts insurers in any way, regardless of materiality, is disproportionate. Instead, incident response and reporting within the supply chain should be focused on incidents that a significant adverse impact on the insurer's operations. This more focused approach would be consistent with the approach of the EU Digital Operational Resilience Act which focuses attention on major incidents rather than all incidents. We suggest amending paragraph 22 (bullet 2) as follows: "Establishes clear processes for identifying, reporting and responding to incidents, including those that affect third- and nth-party service providers that HAVE A SIGNIFICANT ADVERSE impact on the operations of the insurer;"	The proportionality principle would apply here.
88	Institute of International Finance	Yes	In Paragraph 22, the IAIS should focus on critical third-party and nth-party service providers that materially impact the provision of critical services to customers. As currently drafted, Paragraph 22 is overbroad in its approach to service providers that impact the operations of the insurer. The current language of Paragraph 22 could extend to nearly any insurance service provider and is not risk- and materiality-based. We note the focus on service providers that are critical to the insurer's business in Paragraph 26 and recommend a similar focus throughout the Draft Application Paper.	The proportionality principle would apply here.

No.	Respondent	Public Y/N	Comment	Resolution of comment
89	Global Federation of Insurance Associations (GFIA)	Yes	GFIA supports the objective for insurers to effectively manage cyber incidents, including notifications to regulatory authorities and other stakeholders, even if the incident affects third party service providers. This objective is consistent with the US Insurance Data Security Model Law, which provides that if the incident causes material harm, the NAIC Insurance Data Security Model requires notification to the commissioner and to the consumers. The same applies if the breach happens in a system maintained by a third-party service provider. Regarding the second bullet, organisations may not be aware of any incident response/reporting with nth parties.	The proportionality principle would apply here.
90	Financial Sector Conduct Authority (South Africa)	Yes	"nth-party service providers," While this may be appropriate for a specialised audience, translating the term into more straightforward language could make the document more accessible.	No change - this term aligns to terminology used by the Financial Stability Board Toolkit on Enhancing Third-party Risk Management and Oversight. Here, nth-party service providers are defined as "A service provider that is part of a third-party service provider's supply chain and supports the ultimate delivery of services to one or more financial institutions."
91	Liberty, South Africa Insurance Services	Yes	Effective communication remains the cornerstone for ensuring a well-coordinated response to operational incidents. Prioritising robust communication strategies and protocols as part of incident management plans. Visibility of incidents for third and nth parties would require a more robust process as insurers are likely to better manage incidents that is within its control. Ideally incident response plans should be integrated across all relevant stakeholders.	Noted
Comments on Section 2.2.5				

92	Escode (a part of NCC Group)	Yes	Section 2.2.5 should be updated to reflect the role of back-up options such as escrow. Specifically, the following amendment to the text should be made: "In support of this objective, it is important for the insurer to consider how its approach to operational resilience supports a stable and resilient technology environment through appropriate risk management practices, inclusive of its technology architecture, technology asset management, patch management, service monitoring, disaster recovery practices and use of back-up or escrow solutions." Escrow agreements, along with the associated verification testing, are increasingly being built into financial services' risk management and risk control strategies. Escrow agreements enable firms to assume supplier fault by default and cost-effectively mitigate the myriad of risks associated with reliance on third-party providers. Authorities who currently promote or mandate escrow agreements within their third-party risk management (TPRM) frameworks include: • the U.S. Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the Office of the Comptroller of the Currency (OCC) (https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html) • the U.S. Federal Financial Institutions Examination Council (https://ithandbook.ffiec.gov/media/m21ni0b3/ffiec_itbooklet_developmentacquisitionmaintenance.pdf) • the Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/stopransomware/ransomware-guide) • the Bank of England and UK Prudential Regulatory Authority (PRA) (https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf?la=en&hash=5A029BBC764BCC2C4A5F337D8E177A14574E3343) • the Monetary Authority of Singapore (https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf) • the Hong Kong Monetary Authority (https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf) • the Indonesian Otoritas Jasa Keuangan (https://www.ojk.go.id/id/kanal/perbankan/regulasi/surat-edaran-ojk/Documents/SAL%20SEOJK%2021%20-%20MRTI.pdf) • the Reserve Bank of India (https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0) and Securities and Exchange Board of India (https://www.sebi.gov.in/sebi_data/commondocs/jul-2021/Chapter 2 - Trading Software and Technology_p.pdf) • the State Bank of Pakistan (https://www.sbp.org.pk/bprd/2019/C6-Annex-II.pdf) • the Central Bank of Jordan (https://www.cbj.gov.jo/EchoBusv3.0/SystemAssets/PDFs/2021/CSF4JFSv1.0.pdf) • the Reserve Bank of New Zealand (https://www.rbnz.govt.nz/hub/-/media/project/sites/rbnz/files/consultations/banks/outsourcing-policy-for-registered-banks/final-policy-decisions-	Noted.

			outsourcing-policy-registered-banks-feb17.pdf) • the Bank for International Settlements (BIS) Innovation Hub (https://www.bis.org/publ/othp70.pdf) • the Securities Commission Malaysia (https://www.sc.com.my/api/documentms/download.ashx?id=2f253636-07dd-4355-b89e-010b2ef581c1) We would emphasize the difficulties in exhaustively identifying a supplier's risk profile, given it is generally the result of a combination of factors. Identifying all possible scenarios is likely disproportionate to its potential benefits and would likely lead to increasing costs and creating barriers to innovation. For that reason, cloud, software and technology escrow solutions can offer legal, technical and proportional assurance to insurance providers in dealing with their third-party suppliers, particularly where they embrace the concept of 'Resilience by Design'. This would assume supplier failure by default, regardless of their risk profile, and encourage using cloud, software and technology escrow agreements as a proportionate and cost-effective solution for regulated entities to mitigate against this. Indeed, escrow agreements and verification services act as a technical insurance policy and business continuity strategy, safeguarding the long-term availability of business-critical technologies and applications while protecting intellectual property. Establishing cloud, software and technology escrow agreements with supporting verification services creates a baseline to: • Grant organizations access to the source code and the right to access the cloud environment where it is hosted, where: an application is material to the organization's operational continuity, if the service is deployed in the cloud; or if the application presents a concentration risk. Indeed, as stated above, the role of escrow agreements is reflected in CISA's guidance on ransomware (https://www.cisa.gov/stopransomware/ransomware-guide) which states that, in being prepared for a ransomware incident, organizations should ensure the availability of source code through backups or escrow agreements. The details of any access rights and conditions will be set out in individual agreements, offering a legal basis with full transparency for all involved parties over when any such rights can be invoked. • Specify how the agreement and access rights are to be used in the event of supplier compromise or failure. Principally, critical sectors rely on failed services continuing to operate while full recovery plans are being implemented. That means that continuity and exit planning needs to take account of implementation, testing and training times that impact on the ability to exchange or replace products and services expediently, safely and compliantly. • Advance capabilities to automate risk tolerance at the application programable interface (API) gateways level to permit control to gracefully failsafe services or providers who may go out of compliance, removing exposure latency in a real-time digital economy. Many financial firms already use escrow solutions as part of their comprehensive business continuity planning when mitigating supplier risk, and some third party providers themselves have opted to build these solutions into their offer to support their customers' compliance with regulatory requirements. By way of example, Escode has worked with a	

			banking technology provider on developing a cloud escrow solution. The provider's cloud hosted digital banking software-as-a-service (SaaS) solutions supports more than 6,000 loan and deposit products serving over 14 million end customers worldwide. Working with Escode, the provider adopted a cloud escrow solution to establish a robust approach to its customers' regulatory compliance, offering business continuity assurance by ensuring that financial institutions deploying the provider's solution would have access to their application and specific cloud environment as well as support for the ongoing maintenance and management of their application. However, we believe that there is still insufficiently widespread awareness of the benefits of software and technology escrow solutions, and the role they can play in addressing regulatory requirements on outsourcing and third-party risk management. To address this lack of awareness, we believe that there is a role for the IAIS to do more to promote and educate organizations on the benefits of cloud, software and technology escrow solutions as a practical means to meet outsourcing and risk management requirements, as per the suggested amendment to 2.2.5 above.	

No.	Respondent	Public Y/N	Comment	Resolution of comment
93	National Association of Insurance Commissioners (NAIC)	Yes	Revise to reinforce the Board's ultimate responsibility for ensuring that the insurer has effective systems in place and management effectively implements them. The Board ensures the insurer manages and mitigates the impact of technology risk to critical services by implementing an effective approach to operational resilience that addresses the phases of protection, detection, response, and recovery (ICP 8)	More information is now included in the application paper, together with practices.
94	General Insurance Association of Japan	Yes	In light of the NIST (National Institute of Standards and Technology) and other general frameworks, it is appropriate to have "identification" before "protection, detection, response, and recovery".	Agree
95	Global Federation of Insurance Associations (GFIA)	Yes	In light of the NIST (National Institute of Standards and Technology) and other general frameworks, it is appropriate to have "identification" before "protection, detection, response, and recovery". Also, with regards to the language, “Reinforces the adoption and maintenance of good cyber hygiene practices (eg identity management, user authentication practices (such as multifactor authentication), access control, attack surface management etc.)”, GFIA suggests referring to “applicable standards” rather than best practices/ examples.	Agree
Comments on Paragraph 23				
96	National Association of Insurance Commissioners (NAIC)	Yes	Some typos/spacing issues; don’t need etc with eg: • Reinforces the adoption and maintenance of good cyber hygiene practices (eg identity management, user authentication practices (such as multifactor authentication), access control, attack surface management); • Supports regular testing of the approach to operational resilience (including but not limited to cyber resilience) and incorporates effective situational awareness and threat intelligence	Agree

No.	Respondent	Public Y/N	Comment	Resolution of comment
97	General Insurance Association of Japan	Yes	- Paragraph 23 in general is very detailed. In addition, various perspectives are described in parallel in bullet points, making it difficult to understand what kind of response will be required. For example, regarding the first bullet point, what is the intention of selecting these categories among many security measures? If internationally used standards are referred to, we suggest clarifying the source and adding a sentence such as "For example, the following approaches could be considered with reference to...". - Generally, measures by people/policies/technologies are considered to be effective. Based on the premise that this paragraph is intended to provide examples, we suggest adding a policy perspective.	Edits made to objective 2.5 to reduce detail.

No.	Respondent	Public Y/N	Comment	Resolution of comment
98	Global Federation of Insurance Associations (GFIA)	Yes	GFIA supports the objective that requires a robust approach to technology to ensure sensitive and critical information is safely held. This objective is consistent with the US NAIC Insurance Data Security Model Law, which requires each insurer to “Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee’s operations, including: (a) Employee training and management; (b) Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and (c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures.” The Model also requires each insurer to “Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards’ key controls, systems, and procedures.” Regarding the sixth bullet, this item requires additional clarity. The method for testing the “approach to operational resilience” should be clearly defined. Paragraph 23 is overly detailed. In addition, various perspectives are described in parallel in bullet points, making it difficult to understand what kind of response will be required. For example, regarding the first bullet point, what is the intention of selecting these categories among many security measures? If internationally used standards are referred to, we suggest clarifying the source and adding a sentence such as "For example, the following approaches could be considered with reference to...". Generally, measures by people/policies/technologies are considered to be effective. Based on the premise that this paragraph is intended to provide examples, GFIA suggests adding a policy perspective.	Noted - examples of practices to be considered in the development of the Toolkit. Edits made to objective 2.5 to reduce detail.
Comments on Section 2.2.6				

No.	Respondent	Public Y/N	Comment	Resolution of comment
99	National Association of Insurance Commissioners (NAIC)	Yes	Revise to reinforce the Board's ultimate responsibility for ensuring that the insurer has effective systems in place and management effectively implements them. The Board ensures the insurer plans, tests, and implements changes in a controlled manner (ICP 8)	More information is now included in the application paper, together with practices.
100	Global Federation of Insurance Associations (GFIA)	Yes	The focus on controlled changes is appropriate, but the paper does not sufficiently account for the operational challenges insurers face when implementing these changes. Supervisory expectations regarding the testing and implementation of changes should be more clearly outlined, particularly in terms of what is considered “best practice” without imposing burdensome testing requirements that may disrupt ongoing operations. More flexibility in the application of these guidelines would be welcome, especially for smaller firms.	Noted
Comments on Paragraph 24				
101	Escode (a part of NCC Group)	Yes	The requirement to develop “contingency plans” - while welcome - should be expanded to include “stressed exit plans” too. A stressed exit is when the contract is ended due to the failure or insolvency of the service provider, and therefore is more unexpected than a non-stressed exit, which could be due to commercial, performance or strategic reasons. Stressed exit strategies form an important part of business continuity plans, ensuring an insurance firm’s continued provision of important business services and limiting the impact of disruption on the entity, it’s customers and the wider financial market as a whole. Financial regulators globally, such as the UK’s PRA (https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf?la=en&hash=5A029BBC764BCC2C4A5F337D8E177A14574E3343), require financial institutions to develop such plan.	Noted – contingency plans are to encompass business as usual and stressed exit plans.

No.	Respondent	Public Y/N	Comment	Resolution of comment
102	National Association of Insurance Commissioners (NAIC)	Yes	Revise to reinforce the Board's ultimate responsibility for ensuring that the insurer has effective systems in place and management effectively implements them. The Board ensures the insurer develops, implements, tests and updates its BCP and DRP to ensure that it can respond, recover, resume and restore to a pre- defined level of operation following a disruption in a timely manner (ICP 8)	More information is now included in the application paper, together with practices.
103	The Geneva Association	Yes	We also wish to highlight the challenges faced in engaging with third-party service providers. In section 2.2.7, while the IAIS encourages insurers to periodically test the BCPs of third-party providers, we find that many third parties are often unable or unwilling to share their plans for comprehensive testing. To address this, we recommend that the IAIS suggest alternative methods for assurance, such as seeking validation from third-party providers that their BCPs are regularly reviewed, maintained, and tested. This would provide a reasonable degree of assurance while respecting third-party limitations. We also seek clarification on the use of the term “critical third-party” in this paper. The term can be interpreted in two distinct ways: • Systemically Critical Third Parties: Entities whose services are essential to the stability of the entire financial sector (as in the UK and EU frameworks). • Firm-Specific Critical Third Parties: Providers whose services are critical to the operations of an individual firm, as understood by the FSB. Clarifying the IAIS’s intended definition of “critical third-party” will ensure a consistent understanding and application of the recommendations.	Regarding engaging with third-party service providers on testing BCP’s, objective 2.7 makes clear the insurer should involve critical third-party service providers as needed in the insurer’s process to validate that its recovery objectives can be met in a range of severe but plausible scenarios. In this context, consistent with the FSB Toolkit for enhancing Third-Party Risk Management and Oversight, the term critical-third party refers to third-parties that provide critical services to the insurer.

No.	Respondent	Public Y/N	Comment	Resolution of comment
104	Central Bank of Ireland	No	BCP and DR vital tools to keep up to date and how is can differ from Operational Resilience, some clarity to advise firms what is the difference between resilience and B-C Plans. IAIS should consider including, defining the traditional focus of BCP and how it differs to operational resilience. Traditional BCM focuses on single points of failure whereas, operational resilience determines how single points of failure could affect the end-to-end delivery of critical or important business services. Operational resilience is much wider than just business continuity since it requires coordination between risk management, business continuity management (BCM), incident management, third party risk management, Information Communication Technology (ICT) and cyber risk, and recovery and resolution planning.	Noted – more issues are now covered in the Toolkit.
Comments on Paragraph 25				
105	Google Cloud	Yes	Comments on paragraph 25 We assume that the intention of paragraph 25 bullet 3 is to ensure that critical third-party service providers are undertaking appropriate business continuity planning and testing for their own service delivery. The sub-paragraph however may be read as requiring the regulated entity to directly test the service provider's business continuity plans rather than obtain assurance from the service provider that they themselves are testing periodically. An expectation that each regulated entity directly test its service providers' BCPs is extremely operationally challenging in a multi-tenant environment like a public cloud service. This approach could harm operational resilience as testing by one regulated entity has a high risk of impacting the services received by other customers (including other regulated entities). This is particularly the case for more traditional approaches to BCP testing like failover. We suggest amending paragraph 25 (bullet 3) as follows: "Validates that its recovery objectives can be met in a range of severe but plausible scenarios, via periodic testing of BCPs, including THROUGH ASSURANCE THAT CRITICAL THIRD-PARTY SERVICE PROVIDERS CARRY OUT PERIODIC BCP TESTING."	Regarding engaging with third-party service providers on testing BCP's, , objective 2.7 makes clear the insurer should involve critical third-party service providers as needed in the insurer's process to validate that its recovery objectives can be met in a range of severe but plausible scenarios.

No.	Respondent	Public Y/N	Comment	Resolution of comment
106	Institute of International Finance	Yes	The supervisory approach to third-party (and nth-party) service providers should also reflect insurers' limitations on third-party oversight arising from contract terms or market practice. Specifically, insurers can be limited in their ability to validate the business continuity plans (BCPs) of third-party service providers. We would amend the language of the final bullet in Paragraph 25 of Section 2.2.7 to read as follows: Validates that its recovery objectives can be met in a range of severe but plausible scenarios, via periodic testing of BCPs, and, where possible, testing of the BCPs of critical third-party service providers. Where testing of the BCPs of critical third-party service providers is not feasible, insurers should engage with their critical third-party service providers in order to understand their approaches to operational resilience for any critical service they provide to the insurer.	Regarding engaging with third-party service providers on testing BCP's, , objective 2.7 makes clear the insurer should involve critical third-party service providers as needed in the insurer's process to validate that its recovery objectives can be met in a range of severe but plausible scenarios.
107	General Insurance Association of Japan	Yes	- Regarding "clear recovery objectives", is it correct to understand that insurers are to set RPO(Recovery Point Objective), RTO(Recovery Time Objective), etc., which they consider appropriate? - Insurers are not supposed to validate testing of the BCPs of third parties. In this context, is "confirmation of test results" synonymous with "validation"?	Regarding recovery objectives, the insurer and its Board are ultimately responsible for the process undertaken to set these objectives. Regarding engaging with third-party service providers on testing BCP's, objective 2.7 makes clear the insurer should involve critical third-party service providers as needed in the insurer's process to validate that its recovery objectives can be met in a range of severe but plausible scenarios.

No.	Respondent	Public Y/N	Comment	Resolution of comment
108	Global Federation of Insurance Associations (GFIA)	Yes	GFIA supports the objective for insurers to have clear recovery and contingency plans in case of a cyber incident. This objective is consistent with the US NAIC Insurance Data Security Model Law, which requires each insurer to establish a written incident response plan designed to recover from any cybersecurity incident. Regarding the third bullet, it may not be appropriate/feasible for organisations to test the BCPs of its third parties, however it is reasonable to request from the third party the date of the last test and the results. Regarding "clear recovery objectives", is it correct to understand that insurers are to set RPO（Recovery Point Objective, RTO（Recovery Time Objective), etc., which they consider appropriate? Finally, insurers are not supposed to validate testing of the BCPs of third parties. In this context, is "confirmation of test results" synonymous with "validation"?	Regarding recovery objectives, the insurer and its Board are ultimately responsible for the process undertaken to set these objectives. Regarding engaging with third-party service providers on testing BCP's, objective 2.7 makes clear the insurer should involve critical third-party service providers as needed in the insurer's process to validate that its recovery objectives can be met in a range of severe but plausible scenarios.
109	Financial Sector Conduct Authority (South Africa)	Yes	Suggested wording: "Creates detailed contingency plans based on defined impact tolerances to mitigate risks to critical services."	Agree
Comments on Section 2.2.8				
110	National Association of Insurance Commissioners (NAIC)	Yes	Revise to reinforce the Board's ultimate responsibility for ensuring that the insurer has effective systems in place and management effectively implements them. The Board ensures the insurer effectively manages relationships with third-party service providers, including intra-group and nth-party relationships (ICPs 7 and 8)	More information is now included in the application paper, together with practices.
111	General Insurance Association of Japan	Yes	We suggest replacing "manages" with "oversees". (The second bullet point also mentions "Supports effective management...".)	No change - oversight could imply a passive form of management, and the intent is to encourage proactive engagement .

No.	Respondent	Public Y/N	Comment	Resolution of comment
112	Global Federation of Insurance Associations (GFIA)	Yes	Regarding the language, “Supports effective management of the potential impact of disruption throughout the lifecycle of its relationships with third-party, including intra-group and nth- party, service providers. This lifecycle includes planning, due diligence, and selection, contracting, ongoing monitoring and termination”, this requirement covering the entire contract’s life cycle as well as the whole subcontracting chain seems disproportionate and should be limited to material ICT services supporting critical/major functions. GFIA suggests replacing "manages" with "oversees" (The second bullet point also mentions "Supports effective management...".).	No change - oversight could imply a passive form of management, and the intent is to encourage proactive engagement.
Comments on Paragraph 26				
113	Institute of International Finance	Yes	The first bullet of Paragraph 26 in Section 2.2.8 should acknowledge in the text (or, at a minimum, in a footnote) that supervisors should treat in a proportionate manner those intra-group service providers that are subject to well controlled, consistent group-wide policies, procedures and processes that are subject to comprehensive risk management and internal and supervisory oversight.	Proportionality underpins all IAIS application papers. This set out at page 2 and paragraph 15 of this application paper.

No.	Respondent	Public Y/N	Comment	Resolution of comment
114	Global Federation of Insurance Associations (GFIA)	Yes	GFIA supports the objective for insurers to manage effective relationships with third-party service providers to maintain the security of information. This objective is consistent with the US NAIC Insurance Data Security Model Law, which provides that "each [insurer] shall exercise due diligence in selecting its Third-Party Service Provider; and an [insurer] shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider." Regarding the first bullet, what is the industry-wide definition of "intra-group"? Additionally, the most logical way for organisations to ensure the management and oversight of nth parties is to perform due diligence on their third parties to ensure that the third party is also performing due diligence checks on their third parties. Often, third parties are reluctant to share these details, hence nth parties would be likely to refuse sharing especially since there is no legal relationship between the organisation and the nth party. The section on third-party risk management highlights an important area, but there is insufficient clarity on the expectations for managing risks from nth-party providers. Many insurers rely on extensive networks of subcontractors, and the current guidance does not adequately address the practical challenges of monitoring and managing these relationships. More explicit guidelines on what is expected from insurers in terms of oversight, without overburdening them with impractical requirements, would strengthen this section.	No change - the Financial Stability Board Toolkit on Enhancing Third-Party Risk Management and Oversight defines intra-group service provider as "A service provider that is part of a financial institution's group and provides services predominantly to entities within the same group. Intra-group service providers may include a financial institution's parent undertaking, sister companies, subsidiaries, service companies or other entities that are under common ownership or control". Examples of practices relevant to managing risks from the use of third and nth-party service providers to be considered in the development of the Toolkit.

No.	Respondent	Public Y/N	Comment	Resolution of comment
115	Association of British Insurers	No	It can be challenging for firms to map key nth parties as the information surrounding their third parties' key dependencies can be challenging to obtain from the third parties and beyond. Therefore, we urge IAIS and regulators to apply the proportionality principle and support firms in their efforts to obtain this information through secure mechanisms. There is also a need to acknowledge the practical challenges in terms of following the requirements. For instance, there would be a need to assess if mapping 4th and nth parties is achievable and a worthwhile use of time and resources to achieve enhanced resilience.	Proportionality underpins all IAIS application papers, as set out at page 2 and paragraph 15 of the application paper.
116	Liberty, South Africa Insurance Services	Yes	Unless insurers have adequate capabilities to keep track of all third parties and nth party service providers, complying to this can be complex, given the multilayered supply chains making it difficult to trace every nth party. This would also require third parties to have adequate capabilities to keep track of their third parties etc. The further down the chain you go, the less visibility you may have. Thus, it may be impractical to identify every nth party. I would recommend that this be rephrased to require only material nth parties at a minimum.	Proportionality underpins all IAIS application papers. This set out at page 2 and paragraph 15 of this application paper.
General comments on Section 2.3 Objectives for insurance supervisors				
117	National Association of Insurance Commissioners (NAIC)	Yes	Consider including the ICP topic or hyperlinking back to ICP listing in Section 1 for each linked ICP in the subsections.	Agree
118	The Geneva Association	Yes	In terms of the structure of the paper, we recommend that the "Objectives for insurance supervisors" section be moved to the beginning of section two. Given the IAIS's role as a convenor of insurance supervisors, it should prioritise promoting best supervisory practices. Supervisory guidance is vital to sector-wide operational resilience, and elevating this section would emphasise the importance of coordinated supervisory oversight in preventing conflicting regulatory regimes and providing clearer direction for firms.	No change - as all of the content of the Application Paper is applicable to insurance supervisors, the paper is structured such that the Objectives aimed solely at insurance supervisors are presented last.

No.	Respondent	Public Y/N	Comment	Resolution of comment
119	Association of British Insurers	No	Overall, we do agree with the objectives proposed in this consultation. However, we believe it is also crucial to highlight the importance of regulators being pragmatic and proportionate in their approaches to overseeing firms' operational resilience. In particular, regulators should aim to be principles-based and allow harmonisation across jurisdictions when appropriate. This will not only help firms comply as there is a wider understanding of the rules and requirements but will also reduce differences between smaller and larger and better resourced firms operating in several jurisdictions.	Proportionality underpins all IAIS application papers, as set out at page 2 and paragraph 15 of the application paper.
Comments on paragraph 27				
120	Institute of International Finance	Yes	We appreciate the language in Paragraph 27 of the Draft Application Paper that emphasizes supervisory communication, collaboration and cooperation, which should be emphasized throughout the Paper.	Noted - objectives 1 and 2 are aimed at both insurance supervisors and insurers, while objective 3 sets out additional objectives for insurance supervisors.
121	National Association of Insurance Commissioners (NAIC)	Yes	"Overseeing" may not be the best word choice here as it suggests the supervisor is responsible for insurer operational resilience. Suggest "monitoring" or "assessing."	Agreed - overseeing replaced by assessing
122	Global Federation of Insurance Associations (GFIA)	Yes	What is meant by "macro levels"? Please provide a definition.	Reference to "macro levels" deleted.
Comments on Section 2.3.1				
Comments on Paragraph 28				

No.	Respondent	Public Y/N	Comment	Resolution of comment
123	National Association of Insurance Commissioners (NAIC)	Yes	“Siloed” does not need to be in quotations.	Agreed
124	Global Federation of Insurance Associations (GFIA)	Yes	Please define “supervisor” in this context.	The IAIS glossary includes definitions of Group-wide supervisor host and home supervisors and involved supervisors
Comments on Section 2.3.2				
125	The Geneva Association	Yes	We suggest that section 2.3.2 be expanded to focus more on interoperability. Promoting the alignment of operational resilience standards across global regulators should be a key objective, and we encourage the IAIS to use its platform to facilitate greater collaboration among regulators on this issue. This would ensure a more consistent and effective global approach to operational resilience.	The IAIS endeavours to collaborate and promote consistency, where relevant, with international standard setting bodies.
Comments on Paragraph 29				

No.	Respondent	Public Y/N	Comment	Resolution of comment
126	Global Federation of Insurance Associations (GFIA)	Yes	GFIA supports the objectives of supervisors, when appropriate, to share information and cooperate with other supervisors to minimise risk. This objective is consistent with the US NAIC Insurance Data Security Model Law, which provides that "the commissioner may share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 8A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material or other information." GFIA suggests that section 2.3.2 be expanded to focus more on interoperability. Promoting the alignment of operational resilience standards across global regulators should be a key objective, and we encourage the IAIS to use its platform to facilitate greater collaboration among regulators on this issue. This would ensure a more consistent and effective global approach to operational resilience. While the importance of supervisory cooperation is recognised, there is little detail on how this cooperation will be operationalised in practice, particularly regarding the sharing of real-time operational risk intelligence. Insurers would benefit from clearer guidance on how this information exchange will affect their operations and what is expected from them in terms of data sharing or reporting to supervisory authorities. A more detailed framework for cross-border cooperation would help insurers better navigate regulatory expectations.	The IAIS endeavours to collaborate and promote consistency, where relevant, with international standard setting bodies. Regarding the operationalisation of cooperation and information sharing, the IAIS has various forums in place to support such exchanges. Further examples to be considered in the development of the Toolkit.

No.	Respondent	Public Y/N	Comment	Resolution of comment
127	Financial Sector Conduct Authority (South Africa)	Yes	Suggested wording: "Defines its strategy for sharing information and collaborating with other supervisors. This strategy should address and minimize legal barriers and other obstacles to cooperation." The bullet points under each objective are informative but can be wordy. Some phrases could be simplified or broken down into more digestible parts for easier comprehension. General comment: Incorporating visual components such as flowcharts or tables might further clarify relationships between objectives, risks, and actions.	Agreed - edits made to objective 3.2.
Comments on Section 2.3.3				
Comments on Paragraph 30				
128	National Association of Insurance Commissioners (NAIC)	Yes	Typo in the second bullet: Integrates expectations for insurance sector operational resilience...	Agreed
129	General Insurance Association of Japan	Yes	Paragraph 30 (first bullet point): It is important to enhance the resilience of the entire industry through information sharing. On the other hand, because matters related to operational resilience could also provide useful hints to cyber attackers, the scope of stakeholders should be carefully limited as necessary when collaborating and transparently communicating with them. Therefore, we suggest adding "taking into account confidentiality" at the end of the sentence.	Agreed and added to objective 3.3.
130	Global Federation of Insurance Associations (GFIA)	Yes	Regarding paragraph 30 (first bullet point), it is important to enhance the resilience of the entire industry through information sharing. On the other hand, because matters related to operational resilience could also provide useful hints to cyber attackers, the scope of stakeholders should be carefully limited as necessary when collaborating and transparently communicating with them. Therefore, GFIA proposes to add "taking into account confidentiality" at the end of the sentence.	Agreed and added to objective 3.3.

No.	Respondent	Public Y/N	Comment	Resolution of comment
131	Financial Sector Conduct Authority (South Africa)	Yes	Suggested wording: "Engages with stakeholders including the industry, service providers, government agencies, non-governmental organisations, and policyholders on insurers' operational resilience approaches."	No change – terms "third- and nth-party service provider used to align to terminology set out in the Financial Stability Board Toolkit on Enhancing Third-party Risk Management and Oversight.
Comments on Section 2.3.4				
Comments on Paragraph 31				
132	Global Federation of Insurance Associations (GFIA)	Yes	The sentence "Invest in staff training and recruitment to maintain sufficient technical expertise in the areas" should be expanded to include training of staff (including Senior Management) regarding their roles and responsibilities - noted in E-21 s4.1.2 and 4.1.3.	Agreed – updates made to objective 3.4
133	Financial Sector Conduct Authority (South Africa)	Yes	General comment: Including practical examples or case studies of how these objectives might be applied could also enhance understanding.	Noted - material now included in the Toolkit.
General comments on Section 3 Toolkit supporting Objectives for Insurance Sector Operational Resilience (placeholder): Noting that the toolkit is under development and will be published for consultation in 2025, you are invited to share any preliminary comments or highlight any particular issues that you would like to see addressed in a toolkit.				

No.	Respondent	Public Y/N	Comment	Resolution of comment
134	The Geneva Association	Yes	We understand that this document forms part of a two-phase consultation, with the second phase, focusing on the toolkit, expected to be launched later this year. While the current phase provides valuable insight into the IAIS's objectives, we believe that a more comprehensive response from our side will be possible once the toolkit has been released. Given the interconnected nature of these two phases, we are of the view that a complete understanding of the IAIS's approach to operational resilience will only be achievable after reviewing the toolkit. Therefore, we anticipate providing more meaningful and substantive feedback at that time. We look forward to the release of the toolkit and the opportunity it will provide to engage more fully with the IAIS on this topic.	Noted
135	Central Bank of Ireland	No	We are happy to meet and give you a demonstration of our one and that we could learn from each other. Within our toolkit we have the following: Our Guidance An Operational Resilience Curriculum - Principals and how to assess a firms operational Resilience Maturity Assessment Info Requests Supervisory Questions	Noted
136	Association of British Insurers	No	We look forwards to seeing the toolkit. We hope IAIS finds our comments useful and we make ourselves available to discuss them in more detail if helpful.	Noted
137	Old Mutual South Africa	Yes	Inclusion of more detailed guidance on how to go about: - identifying and mapping all critical services, - setting thresholds and testing them (especially non-Tech key dependencies) including examples, - dealing with systemic Financial Services or wider risks which impact operational resilience	Noted