

Resolution of public consultation comments on the Application Paper on operational resilience objectives and toolkit

1-7-25 to 29-9-25

| ID | Organisation | Comment | Resolution of comment |
|---|---|--|---|
| General comments on the Application Paper | | | |
| 1 | Financial Services Commission (FSC) Mauritius | <p>General Remarks</p> <p>We welcome the IAIS's Draft Application Paper on Operational Resilience Objectives and Toolkit as a timely and thoughtful contribution to strengthening the resilience of the insurance sector globally. The paper addresses a broad range of emerging operational risks in a practical and principles-based manner, aligned with the Insurance Core Principles (ICPs).</p> <p>From a Mauritius jurisdiction perspective, we support the IAIS's focus on flexibility, proportionality, and outcome-based objectives. The inclusion of a non-prescriptive toolkit is especially useful for emerging and small jurisdictions such as ours.</p> <p>We offer the following specific comments and suggestions from the viewpoint of a small but open economy with an increasingly digitised financial sector.</p> <p>Proportionality in implementation</p> <p>The draft paper recognises the principle of proportionality but could provide clearer guidance or practical examples for smaller jurisdictions and insurers with limited operational scale.</p> <p><i>Recommendation:</i></p> <p>We suggest the IAIS incorporate a tiered or risk-based application of the toolkit, distinguishing expectations for:</p> <ul style="list-style-type: none"> • Large internationally active insurers (IAIGs) • Medium-sized regional insurers • Small domestic or niche insurers <p>This would ensure practical implementation for markets like Mauritius, where many insurers are small to medium-sized and operate under resource constraints.</p> <p>Supervisory Capacity and Support Tools</p> | <p>Proportionality is built into all of IAIS' work. An addition was made in section 1.1 to reiterate this point.</p> <p>While these changes have not been made in the Application Paper we will reflect some approaches to this in the member only webinars.</p> <p>In terms of capacity building the IAIS will host a series of webinars in Q1 2026 to discuss the Application Paper which will support capacity building. FSC would also be welcome to join the ORWG which will provide the opportunity to share emerging practices.</p> <p>Issues related to data protection and confidentiality were considered during the drafting. Many of the jurisdictions on the drafting team have developed data protection legislation. Considerations on these points will be reflected in the member webinars.</p> <p>As part of the IAIS 2026-2027 Roadmap the ORWG will look at developing a mechanism for gathering data on material operational incidents. The IAIS will then be able to use this data to look at common trends and share supervisory practices with its members.</p> <p>Application Papers generally do not include implementation timelines. However, these issues could also be reflected in the member only webinars.</p> |

| ID | Organisation | Comment | Resolution of comment |
|----|--------------|---|-----------------------|
| | | <p>The broad scope of resilience (cyber, ICT, third-party risk, scenario testing, governance) demands significant supervisory expertise and technical capacity that may not be readily available in smaller jurisdictions.</p> <p><i>Recommendation:</i></p> <p>We encourage the IAIS to:</p> <ul style="list-style-type: none"> • Develop supplementary tools or templates for supervisors • Consider capacity-building initiatives or workshops focused on operational resilience implementation in developing or emerging markets. • Facilitate cross-jurisdictional supervisory collaboration, particularly for shared or common third-party providers. <p>Data Protection and Confidentiality Considerations</p> <p>The Paper refers to data governance in a broad sense, but for jurisdictions like Mauritius with robust data protection laws (e.g., the Data Protection Act 2017), there may be tensions between data access for resilience purposes and legal privacy obligations.</p> <p><i>Proposal</i></p> <p>IAIS may:</p> <ul style="list-style-type: none"> • Provide further guidance on balancing resilience data collection and privacy laws, particularly in the context of: <ul style="list-style-type: none"> ○ Cross-border data flows during disruptions ○ Data sharing between insurers and regulators ○ Use of personal or customer data in resilience testing <p>Legal and Regulatory Alignment</p> <p>The practical implementation of the Paper's objectives may require updates or alignment with local regulations, particularly in areas such as mandatory reporting of disruptions, third-party governance, and business continuity obligations.</p> | |

| ID | Organisation | Comment | Resolution of comment |
|----|--------------|---|-----------------------|
| | | <p><i>Recommendation:</i> We suggest the IAIS:</p> <ul style="list-style-type: none"> • Encourage jurisdictions to undertake a regulatory gap analysis before full adoption. • Provide examples of legal provisions or rulemaking that support effective implementation of resilience principles. <p>Industry Engagement and Information Sharing Comment: Operational resilience benefits significantly from coordinated sectoral responses and shared learnings. Mauritius would benefit from mechanisms that encourage collective sectoral exercises, especially given the limited number of large insurers.</p> <p><i>Proposal:</i> IAIS may:</p> <ul style="list-style-type: none"> • Promote the development of information-sharing frameworks, including anonymised incident reporting between insurers and regulators. • Highlight best practices for sector-wide resilience coordination and mutual aid during system-wide disruptions. <p>Implementation Timeline and Monitoring Given varying jurisdictional starting points, a phased implementation approach with a clear monitoring plan would help supervisors and insurers plan ahead.</p> <p><i>Proposal</i> IAIS may:</p> <ul style="list-style-type: none"> • Develop a recommended implementation roadmap, possibly spanning short, medium, and long-term goals. • Encourage supervisory self-assessments or peer reviews on operational resilience readiness. • Consider future benchmarking studies or comparative surveys among IAIS members. | |

| ID | Organisation | Comment | Resolution of comment |
|----|--|---|--|
| 2 | Global Federation of Insurance Associations (GFIA) | <p>GFIA appreciates the opportunity to provide feedback on the IAIS's draft Application Paper on Operational Resilience objectives and toolkit. Operational resilience is a critical issue for the industry, and GFIA recognises and values the important work being undertaken in this area. GFIA particularly welcomes the IAIS's continued focus on this globally significant topic and the emphasis on fostering cohesion across jurisdictions, which is vital to strengthening resilience across the financial sector. GFIA recognises that there is no single or definitive solution to the challenges of operational resilience and therefore GFIA encourages the IAIS to continue sharing the status of its deliberations with insurers as this work progresses. GFIA supports the paper's recognition of proportionality and risk-based approaches, which are vital given that operational risks vary greatly depending on regional characteristics, company size and business models. However, to enhance clarity, GFIA suggests that the paper provide a clear definition of "operational resilience", given the widespread use of the term in different contexts. While references are often made to technology, cyber and third-party risks, GFIA cautions that singling these out could unintentionally suggest they are the only categories of relevance. Instead, the focus should be on all material operational risks, with particular attention to third parties that support critical processes and services. The inclusion of additional international examples, such as those from Canada's OSFI Operational Risk Management and Resilience Guideline, could also help broaden the perspective. At the same time, GFIA has concerns that certain recommendations may risk expanding supervisory authority beyond current mandates in some jurisdictions, particularly around third-party vendor management and broader operational risks. The paper does not address whether supervisors should have a role in overseeing entities critical to the financial stability of economies, such as major cloud service providers, which is an important question for further consideration. Some recommendations could also result in supervisory micromanagement of insurers' operations at Board level or intrude upon privileged Board-executive management deliberations. Moreover, while the paper sets out outcomes-based principles, these are not always tied closely to materiality or risk, creating the potential for disproportionate expectations. Implementation challenges also arise from the fact that regulators in some jurisdictions may lack the technical expertise to apply the oversight recommendations effectively. Strengthening regulatory technical expertise is essential and should be highlighted more prominently, ideally at the outset of the paper rather than later. In addition, GFIA believes that crisis communication deserves significantly more attention within the guidance. Recent cyber-related disruptions globally have demonstrated how inadequate communication can amplify harm to customers and stakeholders. Crisis communication is not only essential for incident response but also serves as a key mitigant for maintaining trust and ensuring a coordinated and transparent response. In conclusion, GFIA strongly supports the IAIS's ongoing work on operational</p> | <p>Regarding defining "operational resilience" in this paper, given that this Application Paper does not set out new IAIS standards, it would be inappropriate to provide a new definition for a term that might be used or interpreted differently depending on the context.</p> <p>Regarding comments on expanding supervisory authority, micromanagement, and disproportionate recommendations, like all IAIS Application Papers, this paper does not set out new requirements. And like all IAIS material, any guidance or suggestions should be applied on a proportionate basis.</p> <p>Regarding crisis communications, this is likely already captured in objective 2.4.</p> |

| ID | Organisation | Comment | Resolution of comment |
|----|---|--|--|
| | | resilience and appreciates the opportunity to provide feedback. GFIA encourages the IAIS to refine its guidance by clarifying definitions, ensuring proportionality, respecting regulatory boundaries, strengthening supervisory expertise and giving greater prominence to crisis communications. By addressing these areas, the IAIS can further enhance the practicality, effectiveness and global relevance of its work on operational resilience. | |
| 3 | General Insurance Association of Japan | <p>Operational risks vary greatly depending on regional characteristics, company size, etc. Therefore, with the aim of encouraging consistency where possible, we agree to respect jurisdictional differences and take a proportionality and risk-based approach.</p> <p>As the term “operational resilience” is widely used in various fields, and discussions based on this term will continue to be held in the future, we suggest that it be defined in this application paper.</p> | <p>Operational Resilience is part of a wider resilience eco-system within organisations which includes multiple disciplines. Additional text was added to para 1.</p> <p>The focus of the AP is on observed member practices grounded in the ICPs.</p> |
| 4 | National Association of Insurance Commissioners (USA) | <p>Several paragraphs have bulleted lists under them. Some of these lists end in “.” But others end in “;”. Suggest being consistent in how the bulleted lists are structured.</p> <p>IAIS usually uses “supervisor” rather than “authority” or “supervisory authority” – this should be made consistent in paragraphs 34, 49, 50, 58, 59</p> | Agree, changes made. |
| 5 | The Geneva Association | <p>In general, the paper is very well done and represents a comprehensive approach to operational resilience.</p> <p>We welcome the IAIS's articulation of objectives in the Application Paper, which are clear and well-aligned with the needs of supervisors looking to develop capabilities in operational resilience. We also appreciate the references to current jurisdictional practices, which align well with the purpose of application papers. However, we believe that supervisors would benefit from clearer guidance on what ‘good’ looks like across different insurer profiles, and potentially examples of the types of evidence supervisors might seek from firms to assess whether they are in fact resilient. We support a non-prescriptive, outcomes-based approach, in which insurers are able to pursue different methods for attaining operational resilience; but to enable such an outcomes-based system to function effectively, supervisors would benefit from a richer picture of what features would characterise an operationally resilient insurer. This would help avoid a global one-size-fits-all approach whilst supporting meaningful supervisory maturity and development. Without this contextual information, there's a risk the toolkit may fall short of its intended purpose as supervisors seeking to build capability in this area might focus more attention on ensuring that firms have followed the toolkit suggestions to the letter rather than effectively assessing whether the firm is resilient.</p> | <p>Toolkit is based on member survey responses, so we are somewhat limited at this stage to the material we have already collected.</p> <p>No edits made.</p> |

| ID | Organisation | Comment | Resolution of comment |
|----|--|--|---|
| 6 | Institute of International Finance (IIF) | <p>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). We commend the IAIS for completing the two-phase consultation process and integrating the toolkit with the previously consulted objectives, creating a comprehensive and consistent framework for operational resilience in the insurance sector.</p> <p>The IIF has consistently advocated for a principles-based, outcomes-focused approach to operational resilience that promotes interoperability across jurisdictions while respecting local market structures and regulatory frameworks. We are pleased to see that this draft Application Paper maintains this approach and builds upon existing governance and risk management frameworks and reflects input from the insurance industry.</p> <p>We welcome the comprehensive, survey-based development of the toolkit reflecting advanced supervisory practices from many IAIS member jurisdictions. This empirical foundation strengthens the flexible applicability and practical utility of the guidance. The inclusion of diverse implementation approaches from multiple jurisdictions effectively demonstrates how common principles can be applied flexibly within different regulatory and legal frameworks.</p> <p>The IAIS should continue to emphasize that operational resilience remains fundamentally a dynamic risk management discipline and should be the responsibility of insurers, with supervisory oversight proportionate to individual risk profiles. We support the definition in Paragraph 7 of an operationally resilient insurer as one that can "encounter, withstand, mitigate, recover and learn from the impact of a broad range of events" as this aligns with an outcomes-focused approach that leverages existing risk management capabilities. Insurers are risk managers with well-established and comprehensive operational resilience frameworks integrated into their operations and governance structures.</p> <p>The Application Paper should acknowledge alignment with important international initiatives, particularly the Financial Stability Board's work on third-party risk management and operational resilience. This alignment promotes consistency across regulatory frameworks and supports effective supervisory cooperation, particularly for cross-border operations. The toolkit's approach complements ongoing FSB efforts to enhance third-party risk management and oversight across the financial services sector.</p> <p>Any final Application Paper should promote convergence on operational resilience</p> | <p>Regarding FSB alignment, see paragraph 13.</p> <p>Regarding convergence, see paragraph 71, which says "Underpinned by the ICPs, this paper supports supervisors in developing approaches that are consistent with global standards while remaining adaptable to local specificities."</p> <p>Regarding group-wide operational resilience frameworks, this specific focus seems beyond the scope of the paper. The objectives and toolkit are grounded in the ICPs which apply to insurers of all sizes, including groups and legal entities. And the paper is intentionally flexible to accommodate different frameworks and structures, so encouraging group-wide operational reliance frameworks may not be appropriate.</p> <p>Regarding interoperable frameworks, an edit was made to paragraph 8 to reflect this point.</p> |

| ID | Organisation | Comment | Resolution of comment |
|----|--------------|--|-----------------------|
| | | <p>principles and coordination among supervisors, while preserving sufficient flexibility for diverse implementation approaches. Given that insurance groups typically develop group-wide approaches to operational resilience that must function across multiple jurisdictions, regulatory fragmentation poses significant challenges. The Application Paper should encourage supervisors to recognize and accommodate group-wide operational resilience frameworks that are acceptable to group supervisors, rather than imposing conflicting jurisdictional requirements that could undermine the coherence and effectiveness of these enterprise-wide approaches. The toolkit should maintain its focus on material risks and vulnerabilities, ensuring that supervisory expectations are calibrated to the size, complexity, and risk profile of individual insurers. We particularly appreciate that the toolkit employs flexible language such as "can" and "could" rather than prescriptive "should" statements, which enables adaptation to local legal requirements, market conditions, and business realities.</p> <p>The IAIS should promote interoperable jurisdictional frameworks designed to minimize regulatory fragmentation while respecting local legal and regulatory requirements. For insurance groups with cross-border operations subject to both home and host oversight, consistent supervisory approaches and terminology are essential for effective risk management and supervisory coordination.</p> <p>We appreciate the IAIS's commitment to an outcomes and risk-based focused approach that builds upon existing frameworks while providing practical guidance for supervisors and insurers. The integration of real-world supervisory practices into the toolkit creates a valuable resource that can evolve as operational risks and technologies develop.</p> <p>We particularly commend the toolkit's flexible approach that allows adaptation to different market structures, regulatory frameworks, and insurer business models. This flexibility is essential for promoting global convergence on operational resilience principles while respecting jurisdictional specificities and the fundamental differences between insurance business models and those of other financial services sectors.</p> <p>The IIF looks forward to continued dialogue as these principles are operationalized across member jurisdictions. We would be pleased to share additional insights from our members' operational resilience experiences and to discuss any aspects of our response in more detail.</p> <p>Please contact Melanie Idler (midler@iif.com) with any questions.</p> | |

| ID | Organisation | Comment | Resolution of comment |
|--|--|--|-----------------------|
| 7 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | <p>In general, the paper is well written and provides a comprehensive approach to operational resilience. The many references to different jurisdictional practices provide a helpful global overview in relation to how operational resilience frameworks can be implemented and supervised effectively.</p> <p>BILTIR's key feedback is as follows: (i) BILTIR is supportive of operational resilience being recognised as an important aspect of an insurer's Enterprise Risk Management ("ERM") framework; (ii) Senior Management are better positioned to hold more specific roles relating to operational resilience, with appropriate Board oversight; (iii) Operational resilience frameworks should be proportionate to the nature, scale and complexity of the insurer; (iv) In Bermuda, operational resilience is generally already well covered under Bermuda's regulatory and supervisory framework; (v) BILTIR is of the view that both service-oriented and process-oriented approaches are viable approaches for operational resilience; (vi) BILTIR recommends against requiring that mapping results be periodically reported to supervisors. (vii) Requirements in relation to end-to-end oversight of third parties and concentration risk need to be realistic and specifically need to recognise that large third parties that represent concentration risk have considerably more power in determining the contractual relationships with insurers. In addition, there may be no ability to move to a suitable alternative provider; (viii) Clarification is requested on whether the intention of the paper is to place enhanced weighting on cybersecurity.</p> | No edits made. |
| General comments on the Executive Summary | | | |
| 8 | National Association of Insurance Commissioners (USA) | <p>Pg. 4, para 1: Editorial suggestion. The concept and definitions of operational resilience take as a premise the assumption that operational disruptions will occur and thus insurers should consider their tolerance for such disruptions and take this tolerance into account when devising their approach to operational resilience.</p> <p>Pg. 4, para 3: Suggest a slight rephrasing. The Insurance Core Principles (ICPs) establish the importance of insurers having effective risk management and governance processes. This paper supports supervisors and insurers in understanding how to assess and address operational resilience in light of the relevant ICP requirements. To this end, it considers how operational resilience can be embedded into existing risk management and governance frameworks.</p> | Agree, edits made. |

| ID | Organisation | Comment | Resolution of comment |
|--------------------------------------|--|---|-----------------------|
| | | <p>Pg. 4, para 4: Suggest a slight rephrasing and breaking up a rather complex sentence. This Application Paper consists of operational resilience objectives (the objectives) and supporting practices and tools (the toolkit). These two components work in tandem: the objectives provide the basis for a high- level framework for meeting the ICPs, while the toolkit provides supervisors with practical implementation approaches. Such approaches will naturally evolve as risk management practices mature (in general and for a given insurer) and new risks emerge.</p> <p>Pg. 4, para 5: As written, it seems like the ORWG did not also draft the toolkit. Suggest rephrasing. The development of this Application Paper took both a top-down and a bottom-up approach. The objectives were drafted by the Operational Resilience Working Group (ORWG) first, and then it developed the toolkit on the basis of a survey conducted with several IAIS Members from multiple jurisdictions (see the Annex for a list of the participating jurisdictions).</p> <p>Pg. 6, para 17, first bullet: Suggest rephrasing so this makes more sense – “other topics” seems to imply topics that are not the focus of this paper. Legal or supervisory requirements: These are generally principles-based and are often included in requirements on general and specific topics, eg corporate governance, operational risk management, technology/cyber risk management and outsourcing/third-party risk management.</p> | |
| 9 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of these sections as drafted with no comments. | No edits made. |
| General comments on Section 1 | | | |
| 10 | Bermuda International Long-Term Insurers and | BILTIR is supportive of these sections as drafted with no comments. | No edits made. |

| ID | Organisation | Comment | Resolution of comment |
|--|--|---|-----------------------|
| | Reinsurers (BILTIR) | | |
| Comments on Section 1.1 (Background and purpose) | | | |
| 11 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of these sections as drafted with no comments. | No edits made. |
| Comments on Section 1.2 (How ICPs support operational resilience) | | | |
| 12 | Global Federation of Insurance Associations (GFIA) | 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 non-public 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 cybersecurity risks to be included in the enterprise risk management process, requires insurers to stay informed on emerging threats and vulnerabilities, and requires personnel to receive cybersecurity awareness training. | No edits made. |
| 13 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of these sections as drafted with no comments. | No edits made. |

| Comments on Section 1.3 (Objectives and toolkit for insurance sector operational resilience) | | | |
|--|--|---|--------------------------------------|
| 14 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of these sections as drafted with no comments. | Noted |
| General comments on Section 2 | | | |
| 15 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of these sections as drafted with no comments. | Noted |
| General comments on Section 3 | | | |
| 16 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of these sections as drafted with no comments. | No edits made. |
| Comments on Objective 1.1 and toolkit material | | | |
| 17 | Global Federation of Insurance | 1. GFIA agrees with the importance of clearly identifying the roles and responsibilities of Boards and Senior Management in supporting operational resilience. Strong governance is fundamental, and GFIA supports the view that board members must have sufficient | 1. No edits made 2. No edits made |

| | | | |
|----|--|--|---|
| | Associations (GFIA) | <p>knowledge, skills, experience and understanding of operational resilience matters to fulfil their responsibilities.</p> <p>2. However, additional clarity on the criteria for assessing board-level understanding would be helpful to ensure that expectations are practical and measurable.</p> <p>3. At the same time, GFIA cautions against approaches that could impose undue burdens or limit flexibility. For example, while supervisors may wish to set insurer impact tolerances or define critical services in a uniform way, this could deprive companies of the ability to determine for themselves how best to secure alternative measures. Such requirements could also impose enormous costs. Therefore, supervisory approaches should be designed with full consideration of the laws and regulations of each jurisdiction, as well as the scale, complexity and characteristics of each insurance company.</p> <p>4. Similarly, expectations around board responsibilities should allow for proportionality. For instance, GFIA does not agree with the suggestion that boards must outline a communication strategy or that they should always approve critical services and their impact tolerances. These responsibilities may appropriately rest with senior management depending on the regulatory framework and governance structure. Flexibility in allocating responsibilities between boards and management is necessary to ensure effective and efficient governance.</p> <p>5. GFIA also notes that some examples in the paper, such as those from Quebec and the US, are more focused on general risk management than on operational resilience specifically. To strengthen the practical relevance of the toolkit, GFIA recommends drawing from examples that are more resilience-centric, such as the UK's policy statements, the EU's Digital Operational Resilience Act (DORA), the Philippines' BSP Circular and Canada's E-21 Guideline. In addition, GFIA is concerned that the reference in Paragraph 21 to testing competencies of board candidates through interviews or presentations could be interpreted too broadly, leading to excessive burden. If retained, this example should be limited to cases where a significant lack of competency is suspected.</p> | <p>The IAIS has not found it practical to prescribe specific training or knowledge standards for the Board as it would depend on the nature, scale and complexity of the firm's activities (and the level of knowledge and skills demands on the Board, in that context).</p> <p>3. No edits made</p> <p>This is related to Objective 2.1 in the consultation paper. Para 25, 26 and 30 provide sufficient flexibility to the firm in tailoring their critical services and impact tolerances in a manner that is fit-for-purpose to them, individually. The IAIS toolkit is guidance for firms and regulators, who may transpose them into local legislation, taking into consideration local market characteristics.</p> <p>4. No edits made</p> <p>We agree that communication strategies and plan can be devised by Senior Management (rather than the Board), and have proposed to move that requirement from para 18 into para 19 (around Senior Management) in the toolkit.</p> <p>5. No edits made</p> <p>Examples from UK, EU and Canada have been cited in Box 2 of the consultation paper. Interviews and presentations, together with other means of verifying the knowledge and skills of the Board, are just examples of various practices observed by the IAIS among member states. The IAIS does not put weight on the importance or appropriateness of one method over the other, or in what circumstances they may be used.</p> |
| 18 | General Insurance Association of Japan | <p>1. We agree on the importance of identifying the roles and responsibilities of the Board and Senior Management.</p> <p>2. On the other hand, specific approaches to operational risk supervision by supervisors, such as uniformly setting insurer's impact tolerances and critical services, may raise concerns that insurance companies will be unable to decide for themselves about whether</p> | <p>1. No edits made</p> <p>2. No edits made</p> <p>This is related to Objective 2.1 in the consultation paper. Para 25, 26 and 30 provide sufficient flexibility to the firm in tailoring their critical</p> |

| | | | |
|----|---|--|---|
| | | <p>to secure alternative measures, and consequently incur enormous costs. Therefore, such approaches should be established with full consideration of the laws and regulations of each jurisdiction, as well as the scale and characteristics of each insurance company.</p> <p>3. Regarding the first bullet point of Paragraph 21, while we understand it is an example, the statement "Competencies appropriate for the management and conduct of business could also be tested through interviews and candidate presentations" could lead to excessive burden. Therefore, we suggest either deleting it or adding a condition such as "...in cases where a significant lack of competency is suspected".</p> | <p>services and impact tolerances in a manner that is fit-for-purpose to them, individually. The IAIS toolkit is guidance for firms and regulators, who may transpose them into local legislation, taking into consideration local market characteristics.</p> <p>3. No edits made</p> <p>Interviews and presentations, together with other means of verifying the knowledge and skills of the Board, are just examples of various practices observed by the IAIS among member states. The IAIS does not put weight on the importance or appropriateness of one method over the other, or in what circumstances they may be used.</p> |
| 19 | National Association of Insurance Commissioners (USA) | <p>1. Pg. 7, para 18: Editorial suggestion. ...and responsibilities cover matters such as establishing and implementing systems, processes and policies at a high level</p> <p>2. Pg. 7, at the bottom of the page: Suggest the heading "Board Members" be moved down to the next page. Also, add a paragraph number to the first paragraph under "Board Members."</p> <p>3. Pg. 8, top of the page, first bullet: it is not the role of the supervisor itself to establish a risk culture, risk appetite, etc. for an insurer. This puts the supervisor in the role of insurer's Board, which is not appropriate. This should be deleted or reworded if a different point was intended.</p> <p>4. Pg. 10, Box 1: it is not clear in the Qatar example whether the requirements have been issued but have a 1 October effective date or whether they will be issued on that date. Assuming it is the former, suggest: The Qatar Financial Centre Regulatory Authority (QFCRA) has issued requirements (effective 1 October 2025) setting out...</p> <p>5. Pg.10, Box1, add the following example: The National Association of Insurance Commissioners' (NAIC) Market regulation handbook, Financial Condition Examiner's Handbook, and Financial Analysis Handbook provide comprehensive guidelines and tools for assessing the efficacy of corporate governance. Required filings such as Form F (Enterprise Risk Report), ORSA (Own Risk Solvency Assessment), and Corporate Governance Annual Disclosure (CGAD), also support objective 1.1 by emphasizing effective corporate governance, robust risk management</p> | <p>1. edits made</p> <p>Editorial changes with no impact on policy recommendation.</p> <p>2. edits made</p> <p>Editorial changes with no impact on policy recommendation.</p> <p>3. edits made</p> <p>Editorial changes with no impact on policy recommendation.</p> <p>4. edits made</p> <p>Editorial changes with no impact on policy recommendation.</p> <p>5. edits made</p> <p>Editorial changes with no impact on policy recommendation.</p> <p>6. edits made</p> <p>Editorial changes with no impact on policy recommendation.</p> |

| | | | |
|----|--|---|---|
| | | frameworks and strong internal controls. | |
| | | 6. Pg. 11, Box 2: For the Netherlands example, is there a link that could be provided to the expectations they have developed? If not, suggest removing as it is a less helpful example and the box already has a number of them. | |
| 20 | Institute of International Finance (IIF) | We support integration with existing governance frameworks rather than creating parallel structures. However, the Application Paper should avoid overly prescriptive requirements for specific technical expertise at the Board level. Companies should have flexibility in terms of the composition of their Boards. The Board should maintain strategic oversight while delegating operational execution to qualified senior management teams who bear primary responsibility for implementing operational resilience given its broad scope and technical nature. | <p>No edits made</p> <p>Objective 1.1 in the consultation paper has not provided specific technical skill requirements for the Board. It aims to ensure that the Board has the necessary skills and knowledge to oversee and challenge, if required, the implementation of the operational resilience framework by Senior Management, as a matter of first principles.</p> |
| 21 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | <p>1. BILTIR is supportive of Objective 1.1 and provides the below comments on the toolkit.</p> <p>2. BILTIR supports supervisors including operational resilience oversight as a responsibility of the Board within existing frameworks and closely related areas such as business continuity and operational risk. BILTIR recommends that the Paper should not advocate for supervisors to be specific in terms of prescribed roles at the Board level but instead require proper oversight through reporting and robust frameworks that are Board approved, with more specific roles remaining at management or committee level.</p> <p>3. BILTIR's view is that whilst operational resilience is recognised as an important aspect of the ERM framework, operational resilience does not require unnecessary weighting with prescriptive unique requirements around Board responsibilities, given this is generally not required for other areas within ERM that may be of equal importance, depending on the nature of the insurer.</p> <p>4. BILTIR also advocates for risk, size, and complexity considerations to be built more clearly into the paper and would suggest that key areas of oversight, such as: (i) how Board reporting is done; (ii) the metrics involved; and (iii) frequency of reporting, should be clearly left to be determined by the insurers rather than prescribed by supervisors, based on proportionality.</p> <p>5. BILTIR considers communication strategies in relation to risk incidents as already well established and integrated into business continuity and disaster recovery plan requirements, such that it may not be necessary to also have an additional requirement under operational resilience. As such, this item could be removed from the toolkit.</p> | <p>1. No edits made.</p> <p>2. Edits made.</p> <p>The responsibility of the Board in Objective 1.1 of the consultation paper have been rearranged to follow the right sequence of duties and oversight responsibilities of the Board. The requirement for ensuring proper systems and controls has been moved to the next section where joint responsibilities of the Board and Senior Management are discussed.</p> <p>3. No edits made.</p> <p>The IAIS has considered that clear responsibilities of the Board and Senior Management are necessary to stress the importance of governance in operational resilience. The IAIS has seen varied practices in how detailed (or not) general ERM frameworks may be, which – in certain situations – may not explicitly put the necessary weight on operational resilience.</p> <p>4. No edits made.</p> <p>The IAIS has not considered adding specific recommendations in Objective 1.1 related to Board reporting, leaving that to the discretion of individual firms and regulators (in terms of scope, depth and frequency, in commensurate to firm characteristics).</p> |

| | | | |
|---|--|---|---|
| | | <p>6. The Bermuda Monetary Authority ("BMA") already expects Boards to have a range of experiences and skillsets to cover all required aspects of ERM (including operational resilience), and as such, it is BILTIR's view that it is not necessary to have operational resilience as a separate requirement under fit and proper criteria assessments within the toolkit. Furthermore, mandatory interviews of potential Board members specifically on operational resilience matters does not appear necessary although could be required by supervisors on a case-by-case basis. BILTIR also emphasises that it appears reasonable for the management team to have the expertise and the Board to rely upon management, with appropriate oversight and the robust processes that have been Board approved, such that it may not be appropriate to interview Board members to assess expertise in this specific area.</p> <p>7. With regards to the jurisdictional examples provided in Box 1 (page 7), the examples from Quebec and the U.S. appear to be less focused on operational resilience frameworks and are more related to overall risk management and/or operational risk. It is worth noting some regulators (e.g., EU's DORA) made operational resilience very digital, cyber and ICT-centric, unlike others who take a more generalist approach (UK, Canada, Bermuda), making some of these papers difficult to compare scope-wise.</p> | <p>5. No edits made.</p> <p>Following up from an earlier comment, we agreed that communication strategies and plans could be devised by Senior Management (rather than the Board), and have proposed to move that requirement from para 18 into para 19 (around Senior Management) in the toolkit. However, varied practices in this area suggest that explicit mention of communication plans (specific to disruptions of critical services) may go one step forward to encourage proper compliance in this area.</p> <p>6. No edits made.</p> <p>Following up from an earlier comment, interviews and presentations, together with other means of verifying the knowledge and skills of the Board, are just examples of various practices observed by the IAIS among member states. The IAIS does not put weight on the importance or appropriateness of one method over the other, or in what circumstances they may be used.</p> <p>7. No edits made.</p> <p>We agree that country examples in Box 2 are varied, which is one of the reason why the consultation paper has been issued to encourage international harmonisation in this area (with enhanced focus on operational resilience, even where part of the general ERM framework within the firm).</p> |
| Comments on Objective 1.2 and toolkit material | | | |
| 22 | Global Federation of Insurance Associations (GFIA) | <p>1. Although Objective 1.2 states "all risks", each company should be allowed to determine the scope and criteria for identifying risks, taking into consideration the management resources of the insurance companies that identify and manage those risks, as well as the impact and likelihood of occurrence.</p> | <p>1. No edits made.</p> <p>Objective 1.2 in the consultation paper talks about all risks that can severely disrupt the operations of the firm. Immaterial risks of the firm will unlikely have the potential to cause severe disruptions.</p> |

| | | | |
|----|--|---|---|
| | | Regarding paragraph 24: In “Supervisors can require insurers to adopt internal governance and control frameworks that address effective and prudent management of all types of ICT-related risks”, the term “all types of ICT-related risks” is unclear. Therefore, the target should be revised as follows: “...all types of ICT-related risks that have the potential to severely disrupt an insurer’s operations”. | 2. Edits made. Although the original text did not mean to cover immaterial forms of ICT risks, the phrase “all types of” has been deleted to remove the potential for any such connotations. |
| 23 | General Insurance Association of Japan | 1. (Regarding Objective 1.2 "Identifies and manages all risks that have the potential to severely disrupt its operations, including its ability to deliver on its critical services") Although it states "all risks", each company should be allowed to determine the scope and criteria for identifying risks, taking into consideration the management resources of the insurance companies which identify and manage those risks, and the impact and likelihood of occurrence. (Regarding 24 "Supervisors can require insurers to adopt internal governance and control frameworks that address effective and prudent management of all types of ICT-related risks") The term "...all types of ICT-related risks" is unclear, therefore this term should be revised as follows: "...all types of ICT-related risks that have the potential to severely disrupt an insurer’s operations". | 1. No edits made Following up from an earlier comment, Objective 1.2 in the consultation paper talks about all risks that can severely disrupt the operations of the firm. Immaterial risks of the firm will unlikely have the potential to cause severe disruptions. It is not clear to the IAIS the rationale for removing a material risk from the scope of consideration (even where the risk appetite of the firm allows for higher level of risk losses, the identification and assessment of risk is still a necessary part of the risk acceptance or neutralisation mechanism). 2. Edits made. Following up from an earlier comment, although the original text did not mean to cover immaterial forms of ICT risks, the phrase “all types of” has been deleted to remove the potential for any such connotations. |
| 24 | National Association of Insurance Commissioners (USA) | Pg 13, para 22, last bullet: it is not clear how the supervisor itself would integrate operational resilience into an insurer’s ICT risk framework. This puts the supervisor in the role of running the insurer, which is not appropriate. This should be deleted or reworded if a different point was intended. | Edits made. Editorial changes with no impact on policy recommendation. |
| 25 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | 1. BILTIR is supportive of Objective 1.2 and provides the below comments on the toolkit. 2. Regarding supervisors providing additional tools and materials, it is noted that there is a significant amount of local (Bermuda) and global guidance and materials available already such that additional materials may not be necessary for all jurisdictions. 2. BILTIR is supportive of guidance through supervisory events such as information sessions, workshops, seminars or bilateral meetings as this already takes place in Bermuda. Similarly, a combination of self-assessment surveys, on-site inspections, and thematic reviews is already in place in Bermuda. On-site reviews include reviews of meeting | 1. No edits made. 2. No edits made. The IAIS is issuing guidance in this area to fill in the gaps for jurisdiction that have not yet implemented similar standards, and for those may need to harmonise their regime with the common international standards. |

| | | | |
|-------------------------------|--|--|--|
| | | minutes of the Board, the Risk Committee, and other committees. Operational risk management, including operational resilience and information security, is covered by such supervisory efforts and as noted above, may not need to be specifically called out as a standalone area outside of the holistic review of the overall ERM framework. Similarly, the requirement for insurers to identify risks that have the potential to severely disrupt their operations is already a part of the wider business continuity and disaster recovery plans, and BILTIR is of the view it is appropriate for this to remain within the established regulatory framework rather than added as a practice under operational resilience. Separation of duties and three lines of defence is also agreed with as an integral part of the wider ERM framework, which, again, BILTIR considers this should remain as part of holistic efforts. | 2. Following up from an earlier comment, the IAIS has seen varied practices in how detailed (or not) general ERM frameworks may be, which – in certain situations – may not explicitly put the necessary weight on operational resilience. |
| General comments on Section 4 | | | |
| 26 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of these sections as drafted with no comments. | Noted. No edits made. |
| 27 | Global Federation of Insurance Associations (GFIA) | Overall, the main activities of Operational Resilience are described adequately: identification of Critical Operations/Services, dependency mapping, setting of impact tolerances and scenario testing. | Noted. No edits made. |

| Comments on Objective 2.1 and toolkit material | | | |
|--|--|--|---|
| 28 | Global Federation of Insurance Associations (GFIA) | <p>GFIA welcomes the focus on the identification and mapping of critical services and associated resources. GFIA supports the principle that insurers should identify, map, and document critical services, but GFIA encourages the IAIS to allow flexibility in how this is achieved across jurisdictions and company profiles.</p> <p>In addition to the two approaches outlined in the paper, GFIA recommends considering reverse stress testing as another useful option for identifying vulnerabilities and testing resilience.</p> <p>When identifying critical services, GFIA believes that mapping exercises should not only consider operational interconnections but also take into account insurers' management resources, the potential impact of disruptions, and the probability of occurrence. It is also important that insurers retain flexibility in determining the appropriate level of granularity.</p> <p>Regulatory authorities may set expectations, but companies should be able to calibrate the detail of their assessments to ensure they remain proportionate and practical. GFIA notes the challenges associated with identifying interdependencies beyond direct third parties. While due diligence on third parties is an established practice, it is burdensome and impractical for insurers to map dependencies through multiple layers of "nth parties." It should be assumed that a third party is conducting the same due diligence on its own critical service providers, rather than placing this responsibility on insurers. GFIA therefore recommends that the focus remain on the identification of direct third parties that support genuinely critical processes and services.</p> <p>Additional clarity on common criteria used across the industry to identify critical services would also be valuable in promoting consistency. GFIA also notes that the toolkit's reference to bottom-up approaches for identifying critical services could inadvertently result in the over-identification of functions that are not strategically important. This risks diluting resilience efforts by spreading resources too thinly and undermining the focus on genuinely critical activities. Any bottom-up assessments should therefore be carefully calibrated to align with strategic priorities. Similarly, while regulators may find it useful to understand which services are considered critical, the paper does not clearly articulate the benefit of requiring firms to report mapping results regularly. GFIA encourages the IAIS to clarify the</p> | <p>With regards to stress testing, we noted that the testing resilience responses should leverage and consider stressing their critical resources and existing arrangements for recovery and continuity, as well as stress testing. Reverse stress testing is an element of scenario planning.</p> <p>No edits made.</p> <p>On the mapping exercise, noted. Ther IAIS defined high level objectives and provided examples of practices, but it is up to insurers how to achieve these objectives.</p> <p>No edits made.</p> <p>On supply chain mapping, IAIS set high level expectations to identify all interdependencies. Paragraph 60 refers to practice of setting contractual obligations to the 3rd party providers that require them to disclose significant relationships relevant to services provided to insurers, hence identifying relevant nth party providers.</p> <p>No edits made.</p> <p>Noted. The IAIS set high level operational resilience objectives and provided some examples of practices being used. However, the examples do not cover all possible ways to achieve the objectives and insurers should apply practices commensurate with their size, complexity and risk profile.</p> <p>No edits made.</p> |

| | | | |
|----|--|--|--|
| | | supervisory value of such reporting and ensure that related requirements do not create unnecessary burdens. | |
| 29 | General Insurance Association of Japan | <p>In addition to the two approaches for identifying risks and resources, we propose adding the reverse stress testing as another option.</p> <p>The identification of important services should not be limited to the mapping approach, but should include alternatives such as the listing of important services, taking into account the insurance companies' management resources, impact and the possibility of occurrence. In addition, when regulatory authorities specify expected items and items to be included, we believe that each company should retain the flexibility to determine the appropriate level of granularity.</p> | <p>See responses to #28above.</p> <p>No edits made.</p> |
| 30 | The Geneva Association | <p>Objective 2.1 should be broadened to reference both a critical service-oriented approach and a critical process-oriented approach.</p> <ul style="list-style-type: none"> o We believe that both critical service-oriented and critical process-oriented approaches are viable approaches for operational resilience. The service-oriented approach starts by identifying critical business services (outcomes) the company delivers, while the process-oriented approach focuses on critical sequences of activities that make up the insurer's day-to-day operations. o Objective 2.1 currently refers only to critical services. o Suggested wording: Objective 2.1: The insurer identifies and maintains an up-to-date inventory of its critical services <add> and/or critical business processes, with <end add> <remove> and <end remove> interdependencies (ICP 8). <p>In support of this objective, it is important for the insurer to consider how its approach to operational resilience:</p> <ul style="list-style-type: none"> § Ensures an understanding of its critical services or critical business processes, including the resources and risks involved in the delivery of those services; and § Identifies, maps and documents each critical service and/or critical business process end-to-end and the related interdependencies, including, but not limited to, connections with third- and nth-party service providers <p>This wording change would bring Objective 2.1 into alignment with:</p> <ul style="list-style-type: none"> § Paragraph 25, which refers to both a bottom-up (process-oriented) approach and a top-down (service-oriented) approach, § Paragraph 26, which endorses the use of either or a combination of both approaches, and § The jurisdictional examples, which refer to both service-oriented and process-oriented approaches. <p>Also, ICP 8 is arguably more consistent with a process-oriented approach, as ICP 8.2.4</p> | <p>Noted. On the service vs process approach we decided to use critical services definition. Combining service and process will make the objective more confusing. Also, it is difficult to differentiate critical processes from critical services.</p> <p>No edits made.</p> |

| | | | |
|----|--|---|--|
| | | <p>includes a “centralised documented inventory of insurer-wide key processes” as a component of an effective internal controls system.</p> <p>Under objective 2.1, in paragraph 29, the paper refers to the critical processes of “hardware, software, premises, people, other critical processes, third party providers, and materials/supplies, etc.” We believe it is common to refer to “IT systems” instead of hardware and software and to include data (or information) among the critical processes.</p> | <p>Noted. Edits made. Wording of paragraph 29 has been updated to include IT systems and Data.</p> |
| 31 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | <p>BILTIR is supportive of Objective 2.1 and provides the below comments on the objectives and toolkit.</p> <p>Objective 2.1 currently refers only to critical services. BILTIR views that both service-oriented and process-oriented approaches are viable approaches for operational resilience. The service-oriented approach starts by identifying critical business services (outcomes) the company delivers, while the process-oriented approach focuses on sequences of activities that make up the insurer’s day-to-day operations.</p> <p>BILTIR also suggests amendment to the wording of the objective by the following underlined text:</p> <p>Objective 2.1: The insurer identifies and maintains an up-to-date inventory of its critical services and/or business processes, with and interdependencies (ICP 8).</p> <p>In support of this objective, BILTIR considers it important for the insurer to consider how its approach to operational resilience:</p> <p>Ensures an understanding of its critical services or business processes, including the resources and risks involved in the delivery of those services; and</p> <p>Identifies, maps, and documents each critical service and/or business process end-to-end and the related interdependencies, including, but not limited to, connections with third- and nth-party service providers”</p> <p>This suggested wording change would bring Objective 2.1 into alignment with the following: (i) paragraph 25, which refers to both a bottom-up (process-oriented) approach and a top-down (service-oriented) approach; (ii) paragraph 26, which endorses the use of either or a combination of both approaches; and (iii) the jurisdictional examples, which refer to both service-oriented and process-oriented approaches.</p> | <p>Noted. Please refer to response in #29. No additional edits made.</p> |

| | | |
|--|---|--|
| | <p>Under objective 2.1, in paragraph 29, the paper refers to the critical processes of “hardware, software, premises, people, other critical processes, third party providers, and materials/supplies, etc.” We believe it is common to refer to “IT systems” instead of hardware and software and to include data (or information) among the critical processes.</p> <p>In relation to supervisors issuing relevant guidance to explain how insurers can approach the identification of critical services and interdependencies, this is not deemed necessary by BILTIR and should sit with management who understand the business, particularly as this will differ significantly between insurers based on size and complexity. However, details on common criteria used to identify critical services could be helpful if defined and provided by the IAIS.</p> <p>BILTIR recommends against requirements for reporting of results of mapping on a periodic basis to supervisors. For many jurisdictions this would be a significant amount of data going to a supervisor such that it would unlikely be helpful, as the level of review required by the supervisor would not be possible. In addition, supervisors have significant oversight through controls already in place (including existing reporting requirements and on-sites reviews referred to above). Overall, it does not appear that these reporting requirements would bring enough benefit to justify the regulatory compliance burden it would introduce. If this is to be included, BILTIR recommends the paper makes clear that it would only be for critical (or material) service providers. More specific considerations on how to approach periodicity of refreshes/updates (e.g., of mapping) would be helpful as well as confirmation this should be determined based on nature, size and complexity would be beneficial to stakeholders.</p> <p>BILTIR considers that having supervisors issue guidance that specifies expectations for mapping of critical supervisor services and what should be included may be too prescriptive and specific. This is because such guidance often becomes a supervisory expectation rather than guidance, and all areas listed in the examples may not be required (or appropriate) for all insurers based on size and complexity.</p> | <p>Noted. Is up to a supervisory authority to issue such guidance or not depending on the existing regulatory framework. No edits made.</p> <p>The selection of practices and tools included in the toolkit can be implemented according to the specific context and needs of each supervisor and market. The requirement to share results of the mapping with supervisors is an example of regulatory practices used in some jurisdictions. While some jurisdictions may find it too burdensome, other can find benefits of such information to inform supervisors of composition of important services or third party providers concentration. No edits made.</p> <p>Noted. No edits made.</p> |
|--|---|--|

| Comments on Objective 2.2 and toolkit material | | | |
|--|---|--|--|
| 32 | Global Federation of Insurance Associations (GFIA) | GFIA agrees that, given the risk characteristics of operational resilience, a flexible approach should be taken when measuring impacts on insurance companies. Prescriptive or uniform requirements could create unnecessary burdens and may not reflect the diverse risk profiles, business models, and jurisdictional frameworks across the global insurance sector. At the same time, GFIA believes that further examples and explanations of non-prescriptive approaches would be helpful to illustrate how flexibility can be applied in practice, while still ensuring consistency of outcomes. Such clarification would assist insurers in implementing these measures in a way that is both proportionate and effective. GFIA supports the reference in the toolkit to the concept of intolerable harm for consumers, which provides a useful benchmark for setting impact tolerances. GFIA also recognises that, in some jurisdictions such as the UK, the setting of impact tolerances has become a business-as-usual expectation for insurers. While this approach offers a good foundation for strengthening resilience, GFIA notes that firms often face challenges in practice, including metric-based difficulties and interpreting feedback from supervisors. These challenges highlight the importance of supervisory flexibility and open dialogue between insurers and regulators to ensure that impact tolerances are both meaningful and practical. | Noted. No edits made. |
| 33 | General Insurance Association of Japan | Considering the risk characteristics of operational resilience, we agree that a flexible approach should be taken when measuring the impact on insurance companies. On the other hand, examples and explanations of non-prescriptive approaches should be provided from the perspective of the burden that may arise on the insurer that takes such measures. | Noted. No edits made. |
| 34 | National Association of Insurance Commissioners (USA) | Pg. 19, Box 7: Add link to OSFI guidance. | Noted. Link provided. Edits made. |
| 35 | Institute of International Finance (IIF) | While we support the principle that insurers should define the maximum tolerable level of disruption for critical services, we question whether detailed explanations of how impact tolerances relate to wider risk tolerance frameworks would provide meaningful supervisory value. Beyond acknowledging that maximum tolerable disruption levels will exceed normal risk tolerance thresholds, additional elaboration may not offer substantive insights while adding unnecessary complexity to operational resilience frameworks. | Noted. The Application Paper was deliberately drafted in a way that allows for flexibility and proportionality. The paper does not go into any more detail and makes the point about the importance of the coherence with the ERM framework. No edits made. |

| | | | |
|---|--|--|--|
| 36 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of this section as drafted with no comments. | Noted. No edits made. |
| Comments on Objective 2.3 and toolkit material | | | |
| 37 | Financial Services Commission (FSC) Mauritius | <p>Scenario Testing and Impact Tolerances</p> <p>While scenario-based testing is an essential component of operational resilience, insurers in Mauritius may face challenges in designing and executing complex scenarios due to data, expertise, or cost limitations.</p> <p><i>Proposal</i> IAIS may:</p> <ul style="list-style-type: none"> • Provide standardised or baseline scenarios for voluntary use by small insurers. • Offer guidance on how to determine proportionate impact tolerances based on insurer size and market relevance. • Clarify expectations around the frequency and reporting of such testing to supervisors. | <p>These issues will be picked up in a dedicated webinar on scenario testing and impact tolerance as part of the member-only webinars.</p> <p>No edits made.</p> |
| 38 | Global Federation of Insurance Associations (GFIA) | GFIA supports the objective for insurers to understand the potential damage that a disruption in critical services can cause. This aligns with existing frameworks such as the US NAIC Insurance Data Security Model Law, which requires insurers to assess both the likelihood and potential damage of threats while considering the sensitivity of non-public information. GFIA agrees with the principle of testing impact tolerances and third-party arrangements, as such exercises can provide meaningful insights into resilience capabilities. However, GFIA emphasises that proportionality is essential, as smaller firms often face significant challenges in engaging systemic third-party providers in testing exercises. Supervisors should remain mindful of these challenges and allow for proportionate approaches that avoid undue burden. With respect to frequency, GFIA believes that scenario testing should not be prescribed as an annual requirement in all cases. Instead, the frequency should reflect the insurer's risk profile, scale, and | Noted. We agree that the proportionality is essential and to achieve this defined high level operational resilience objectives. Practices and guidance are designed to illustrate how the objectives can be achieved but are not prescriptive nor limit practices to those described in the paper. |

| | | | |
|----|--|---|---|
| | | <p>circumstances, including whether there have been environmental changes, the likelihood and impact of relevant risks, and the operational resources available. For non-critical services, simple walk-through tests may be more appropriate than full scenario testing. A flexible, proportionate approach would allow insurers to maintain focus on the most critical exposures while managing testing burdens effectively. GFIA welcomes the inclusion of impact tolerance setting within Objective 2.2 and notes that, for UK-based insurers, this is already an established expectation. While the integration of these practices into business-as-usual operations provides a strong foundation for resilience, GFIA notes that firms continue to face practical challenges in developing meaningful metrics and in interpreting supervisory feedback. In this regard, GFIA highlights the value of collaborative forums, such as the UK's Cross Market Operational Resilience Group, which bring together firms, supervisors, and policymakers to address common challenges and share regulatory updates. GFIA strongly supports the promotion of such public-private partnerships as a model for fostering shared understanding and progress in this area. Finally, regarding Box 7, GFIA recommends clarifying that CBEST should be referenced as a tool that can help shape firms' understanding of their impact tolerances, rather than as a formal requirement to establish them. In the UK, the obligation to define impact tolerances is set out by the PRA and FCA, and it would be helpful for the toolkit to reflect this distinction more clearly.</p> | <p>With reference to CBEST, this is an observed practice rather than one of the objectives. No edits made.</p> |
| 39 | General Insurance Association of Japan | <p>Although it is described as an "annual" scenario test, the frequency should be determined based on factors such as whether there have been any major environmental changes, the impact and likelihood of risks, the operational resources of insurance companies, and the burden on insurance companies which are to conduct the tests.</p> | <p>Noted. Paragraph 36 in section on frequency of testing already states that "Insurers could perform these exercises more frequently if required (for example, in case of a material changes to critical processes or external environments)". No edits made.</p> |
| 40 | National Association of Insurance Commissioners (USA) | <p>Pg. 20, Box 8: move the box heading down to the next page.</p> <p>Pg. 22, Box 9: add link to DORA reference.</p> | <p>Noted. The text will be formatted before publication. Edits made – link to DORA added in the Box 9.</p> |
| 41 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | <p>BILTIR is supportive of Objective 2.3 and provides the below comments on the referenced practices.</p> <p>BILTIR strongly supports the suggested practice of allowing for proportionality and firm size adjustments. Such an approach should continue to support flexibility, and the setting of risk scenarios should remain a responsibility of each firm rather than having risk scenario parameters prescribed by supervisors.</p> <p>BILTIR notes that there would be practical difficulties in implementing requirements around</p> | <p>Noted. The paper provides a set of examples that can be used to manage testing and self-assessment, but provides sufficient proportionality for insurers to use methods commensurate with their size, complexity, risk profile and business processes.</p> <p>No edits made.</p> |

| | | | |
|---|--|--|--|
| | | <p>end-to-end testing and third parties. Often, such third parties may be large organisations (for example, Amazon Web Services) that are not going to be willing to share or amend resilience testing plans or have obligations imposed upon them, including audit rights. Instead, reliance on contractual terms that requires ERM, business continuity and disaster recovery plans to be in place is most commonly relied upon and deemed sufficient for the required purpose.</p> | |
| Comments on Objective 2.4 and toolkit material | | | |
| 42 | Global Federation of Insurance Associations (GFIA) | <p>GFIA supports the objective of ensuring that insurers can effectively manage cyber and other operational incidents, including those that involve third-party service providers. This aligns with frameworks such as the U.S. Insurance Data Security Model Law, which requires notification to regulators and consumers if an incident causes material harm, even when the breach occurs within a third-party system. GFIA agrees that timely reporting to supervisors and other stakeholders is an important component of incident management, but it must be carefully balanced against the immediate need to contain the incident, understand its causes, and mitigate its impacts. Reporting requirements should therefore be designed to support, rather than hinder, firms' ability to respond effectively to critical incidents. Alignment of reporting frameworks across jurisdictions and regulatory bodies would also help reduce duplication and provide greater clarity for insurers during high-pressure situations.</p> <p>GFIA notes that the paper refers to jurisdictions relying on "implicit requirements" regarding reporting to both internal and external stakeholders, including supervisory authorities. To avoid ambiguity, it would be helpful for the IAIS to provide specific examples of what is meant by "implicit requirements" and how they are expected to operate in practice.</p> <p>In addition, while it is appropriate to require firms to ensure that direct third-party providers are included in incident reporting processes, it would be impractical and unduly burdensome to extend such obligations to nth parties, where insurers have no direct contractual leverage.</p> <p>GFIA also observes that Objectives 2.4 to 2.8 address risk areas that may or may not fall directly within the scope of "operational resilience," depending on how individual regulators structure their frameworks. While these areas are always important pillars of resilience, they are often addressed in separate regulatory papers or guidelines, which can create grey areas of ownership and integration. GFIA therefore recommends that the IAIS acknowledge</p> | <p>On the consistency of incident reporting, the paper provides examples of regulatory practices related to identifying, assessing, reporting and responding to incidents, including those affecting third- and nth-party. However it is up to individual regulators what expectations should be set depending on a jurisdiction's existing practices and regulatory framework.</p> <p>The paper also provides a reference to FSB FIRE Incident reporting framework designed to improve the consistency of incident reporting and encourages regulators to use FIRE.</p> <p>No edits made.</p> <p>On the "implicit requirements" in para 41 (now para 45), "implicit" was deleted.</p> <p>We expect notification requirements to be extended down the supply chain through appropriate contractual obligations. No edits made.</p> <p>Noted. Sections 2.4 to 2.8 are key elements to ensure sound approach to operational resilience and are consistent with other sectors operational resilience guidance (e.g. BCBS Principles for Operational Resilience). No edits made.</p> |

| | | | |
|---|--|--|--|
| | | <p>this variability and highlight the importance of coordination across supervisory frameworks to ensure consistency and avoid overlap.</p> <p>With regard to paragraphs 40–42, GFIA notes that while the heading refers to identifying, assessing, reporting, and responding to incidents, the text largely discusses reporting. It would be useful to clarify where firms can learn from incidents and how lessons should be integrated into resilience planning. GFIA encourages the IAIS to expand its guidance to reflect the full lifecycle of incident management, from detection through containment, reporting, resolution, and post-incident learning.</p> | <p>The example in Box 9 from DORA sets out how financial institutions should learn lessons from incidents.</p> |
| 43 | General Insurance Association of Japan | <p>It is stated that jurisdictions can rely on implicit requirements on their reporting to both internal and external stakeholders, including supervisory authorities, as appropriate. In this context, it would be beneficial to provide specific examples of what is meant by “implicit requirements”.</p> | <p>On the “implicit requirements” in para 41, “implicit” was deleted (now para 45).</p> |
| 44 | National Association of Insurance Commissioners (USA) | <p>Pg. 23, para 41: Justify the first word in the paragraph.</p> | <p>Noted</p> |
| 45 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | <p>BILTIR is supportive of this section as drafted with no comments.</p> | <p>Noted. No edits made.</p> |
| Comments on Objective 2.5 and toolkit material | | | |
| 46 | National Association of Insurance Commissioners (USA) | <p>Pg. 25, Box 11: Add link to Quebec reference.</p> | <p>Link added.</p> |
| 47 | Global Federation of Insurance Associations (GFIA) | <p>GFIA believes that the importance of critical services, change management, and third-party dependencies should be more clearly emphasised in this section. Strengthening the link between broader technology risk activities and these three core aspects is essential to ensuring that resilience efforts are appropriately targeted and effective. Clearer alignment</p> | <p>Noted.</p> <p>The paper underlines the importance of these areas by including into the “Key elements of a sound approach to operational resilience”.</p> <p>The objectives provide the basis for a high-level framework for meeting the ICPs, while the toolkit provides supervisors with practical</p> |

| | | | |
|---|--|--|---|
| | | would help firms better prioritise resources and enhance their ability to manage technology-related risks in a way that supports overall operational resilience. | implementation approaches that will naturally evolve as risk management practices mature (in general and for a given insurer) and new risks emerge. No edits made. |
| 48 | The Geneva Association | Under Objective 2.5, paragraphs 44 and 45, which address the management of technology risks relevant to operational resilience, could be strengthened by one or more references to prominent jurisdictional frameworks such as the Digital Operational Resilience Act (DORA) and the NIST Cybersecurity Framework (NIST CSF). o Cybersecurity is arguably the predominant technology risk relevant to operational resilience, yet paragraphs 44 and 45 currently give it only a minor emphasis. | Noted. While cyber is a significant part of the range of ICT risks, the paper focuses on all aspects of ICT risk management and states that supervisory guidance can extend beyond cyber security. We referred to DORA throughout the paper and want to maintain a balanced set of references. While NIST CRF is one of recognised standards we only referred to practices identified throughout the survey responses. Relevant ISO standards, or COBIT objectives can also be helpful in designing a sound ICT risk management framework. No edits made. |
| 49 | Institute of International Finance (IIF) | We welcome the comprehensive coverage and support the technology-neutral approach that accommodates diverse IT architectures. This flexibility is essential given the differing use of technology and IT infrastructure across different insurers and markets. | Noted. No edits made. |
| 50 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of Objective 2.4 and provides the below comments on the toolkit. BILTIR considers that the paper could be enhanced with clarity on whether cybersecurity is the intended focus or is viewed only as one element (with no more importance) with the operational resilience program under ERM. For example, it is noted that the concepts of protection, detection, response, and recovery are very cybersecurity focused and may not be applicable to operational resilience more widely. Such concepts may be too restrictive in that they may force insurers to adopt a particular model that does not consider resilience exposures outside of cybersecurity. If the intention is to place enhanced weighting on cybersecurity as a risk factor within ERM, it is recommended that the paper make clear where practices are specific to cybersecurity only and place more emphasis on prominent jurisdictional frameworks such as the DORA and the NIST Cybersecurity Framework ("NIST CSF"). | Noted. Cyber security is part of technology risk management, and its weight will depend on an insurer's size, complexity and risk profile. We referred to DORA throughout the paper and want to maintain a balanced set of references. While NIST CRF is one of recognised standards we only referred to practices identified throughout the survey responses. Relevant ISO standards, or COBIT objectives can also be helpful in designing a sound ICT risk management framework. No edits made. |
| Comments on Objective 2.6 and toolkit material | | | |
| 51 | General Insurance | While we agree that it is important to conduct a risk impact analysis in advance when changing operating rules within the operational risk management framework, we believe | Noted. No edits made. |

| | | | |
|---|--|--|--|
| | Association of Japan | that the level of risk to be recognized and the assessment of the analysis results should be left to the discretion of the insurance company. | |
| 52 | Global Federation of Insurance Associations (GFIA) | While GFIA agrees that it is important to conduct a risk impact analysis in advance when changing operating rules within the operational risk management framework, GFIA believes that the level of risk to be recognised and the assessment of the analysis results should be left to the discretion of the insurance company. | Noted. No edits made. |
| 53 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of this section with the recommendation to remove reference to supervisors providing guidance about the scope and frequency of expected reviews that insurers must carry out to improve their change management capabilities. Scope and frequency are considered to be more appropriately set by insurers, again taking into account size and complexity (that is, proportionality). | Removed sentence in para 47 ("In their supervisory materials, supervisors may wish to provide guidance about the scope and frequency of expected reviews that insurers must carry out to improve their change management capabilities.") |
| Comments on Objective 2.7 and toolkit material | | | |
| 54 | National Association of Insurance Commissioners (USA) | Pg 28, Objective 2.7: suggest spelling out BCP and DRP. Pg. 29, para 52: should the paragraph following 52 be numbered? | Noted. Respective edits made. |
| 55 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of this section with the recommendation that risk assessments are not required to be submitted to supervisors. The requirement to conduct the assessments (which is accepted as appropriate), coupled with on-site reviews and supervisors' powers to request such information, would appear sufficient to achieve the objective without adding further reporting compliance obligations. | Noted. It is up to a specific regulator to decide what practices they use. No edits made. |

| Comments on Objective 2.8 and toolkit material | | | |
|--|--|---|--|
| 56 | Financial Services Commission (FSC) Mauritius | <p>Integration with Third-Party and Cross-Border Service Risks</p> <p>Many Mauritian insurers rely on outsourced ICT services, cloud computing, and administrative support (actuarial services) from foreign service providers. The draft paper recognises these dependencies but further clarity is needed on regulatory reach and enforcement options in such cases.</p> <p><i>Recommendation:</i> Our proposal for the IAIS is to:</p> <ul style="list-style-type: none"> • Elaborate guidance on managing cross-border outsourcing, including data residency, service level agreements (SLAs), and legal jurisdiction. • Highlight model contractual clauses that can support resilience (e.g., audit rights, exit strategies). • Provide more detail on how supervisors can ensure compliance and continuity with limited extraterritorial power. | <p>These suggestions will be picked up as part of the ORWG's future work on third parties.</p> <p>No edits made.</p> |
| 57 | General Insurance Association of Japan | <p>In light of the increase in outsourcing to third parties and the rise of cyber risks, we agree to the importance of strengthening supervision of third-party service providers. However, when supervisors are granted the authority to access and audit third-party service providers, as same level as insurance companies have, it is desirable to establish applicable standards and criteria after careful consideration in light of each jurisdiction's laws and regulations.</p> <p>In the case of international third-party service providers such as platform providers, it may not be possible to find alternatives, and a coordinated approach of multiple jurisdictions' supervisory authorities will be necessary. Therefore, we believe it is appropriate to strengthen cooperation not only within the insurance industry but also across the entire financial sector and between multiple industries.</p> | <p>Noted. The practice of insurers and their regulators being able to have effective access to third party service providers is a common approach across all sectors similar requirements and included in respective guidelines (eg FSB toolkit for enhancing third-party risk management and oversight). No edits made.</p> |
| 58 | Global Federation of Insurance Associations (GFIA) | <p>GFIA supports the objective for insurers to manage effective relationships with third-party service providers to maintain the security of information. This aligns with the US NAIC Insurance Data Security Model Law, which requires insurers to exercise due diligence when selecting third party service providers and to ensure that those providers implement appropriate administrative, technical, and physical measures to protect information systems</p> | <p>Noted. Changes made to remove reference to “supply chain”.</p> <p>With regards to nth party management, insurers are expected to manage impact of incidents in nth parties that have significant impact on services provided by third parties. To support this, the paper notes</p> |

| | | | |
|----|---|---|--|
| | | <p>and non-public information. At the same time, GFIA notes that managing the impact of disruptions caused by nth parties would be onerous without a legally binding agreement in place, and therefore supervisory expectations should take this into account. GFIA also recommends consistent use of the term “third party” (which could encompass providers of goods or services) instead of interchangeable terms such as “supply chain,” which may introduce ambiguity. It is important to acknowledge that contracts with third parties are negotiated in competitive environments and sometimes with multiple jurisdictional and/or sectoral regulatory expectations. Insurers may lack sufficient leverage to impose requirements on large or highly concentrated providers, and in these cases GFIA believes they should focus on negotiating in their best interests while implementing appropriate monitoring and processes where contractual terms fall short. A one-size-fits-all approach is not suitable, as risks vary significantly across different types of third-party relationships. Supervisory frameworks should recognize these variations and avoid creating undue burdens that may be impractical for insurers, particularly smaller firms. Given the growth of outsourcing and the heightened cyber risk environment, GFIA agrees that strengthening supervision of third-party service providers is important. However, where supervisors are granted authority to access and audit third-party providers, applicable standards and criteria should be carefully developed in light of jurisdiction-specific legal frameworks. For global providers, such as major platforms where alternatives may not exist, a coordinated supervisory approach across jurisdictions and even across industries will be essential to ensure resilience. Supervisors should also remain mindful of the challenges insurers face in managing these relationships, especially when third parties are not subject to direct regulation and hold significant market leverage. The UK’s forthcoming designation of critical third parties may help to address transparency and collaboration, but it remains uncertain whether this will deliver the intended improvements. GFIA believes supervisory expectations should reflect these dynamics, acknowledging the limitations firms face while still supporting effective relationship management as an integral part of operational resilience.</p> | <p>importance of appropriate contractual obligations being cascaded down to supply chain. On the proportionality and strengthening approach to third-party risks management IAIS supports FSB toolkit on outsourcing and third-party relationships. No edits made.</p> |
| 59 | National Association of Insurance Commissioners (USA) | <p>Pg. 30, para 53: for consistency use “Supervisory practices” rather than “Regulatory practices”.</p> <p>Pg. 31, para 58: as this may not necessarily be a systemic risk, suggest softening: To have a better understanding of, and to mitigate for, this potential systemic risk, jurisdictions may consider granting the supervisor powers to directly oversee the provision of services to financial institutions by critical third-party providers.</p> | <p>Noted. “Regulatory practices” replaced with “Supervisory practices”</p> <p>Added “potentially”</p> <p>Edits made.</p> |

| | | | |
|----|--|--|--|
| 60 | Institute of International Finance (IIF) | <p>The IAIS should focus on critical third-party service providers (TPSPs) that materially support the delivery of services that are critical to the insurer's continued operation. We recommend defining critical TPSPs as service providers that support to a material extent the provision of services that are essential to the insurer's business continuity.</p> <p>The supervisory approach should recognize that while insurers remain responsible for managing all risks that may impact their operations, including those arising from nth-party providers, they should not be expected to manage risks that impact nth parties until those risks materially affect the insurer's operations. This distinction is important for maintaining appropriate accountability while acknowledging the practical limitations of direct oversight capabilities. Market dominance and specialization of some vendors create practical constraints that supervisors should consider when setting expectations, while recognizing that insurers maintain responsibility for understanding and mitigating the impact of third-party dependencies on their own operations.</p> <p>We continue to believe that intragroup services should be treated differently than external third parties where they are subject to consistent group-wide governance and controls. The provision of services on an intragroup basis should benefit from recognition of enhanced oversight capabilities where robust, globally consistent policies, procedures, and processes are in place.</p> | <p>Noted.</p> <p>The objective of this section is an effective management and oversight of supply chain risks; Insurers should decide which service providers are critical to the delivery of their critical services. No edits made.</p> |
| 61 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | <p>BILTIR is supportive of the objective and oversight over third-party service providers but repeats the comments under paragraph 7 above regarding the difficulties in practical implementation.</p> <p>In particular, involvement of third parties in operational resilience activities (mapping of nth parties, participation in testing) is often controversial because supervised firms do not have the leverage to contractually ask more of highly concentrated, large suppliers. BILTIR understands that such problems have arisen under DORA, with reports from insurance groups operating in the EU reporting that large organisations, that would be deemed critical service providers, not being willing to submit to such requirements.</p> <p>An alternative is to bring critical third-parties under the supervisory powers of the regulatory authority (for example, as under the UK's "CTP Oversight Regime") instead of having financial institutions shoulder the burden alone. However, BILTIR considers that whilst this scenario is better than placing the burden on the insurers, it is new and we understand there have been mixed results with implementation observed.</p> <p>In which case, it is recommended to remove the references from the paper to such</p> | <p>Noted.</p> <p>We note that supervisory practices on outsourcing are relatively advanced, and jurisdictions have matured their approaches in recent years. Third-party risk management is an evolutionary advancement of practices on outsourcing and looks at management of relationships with third-party service providers more holistically. As such these practices remain largely effective.</p> <p>We recognise the increased concentration risk from insurers' use services from a limited number of large third-party service providers. We therefore suggested in paragraph 59 jurisdictions to consider granting supervisory authorities powers to directly oversee the provision of services to financial institutions by critical third-party providers. No edits made.</p> |

| | | | |
|-------------------------------|--|---|---|
| | | <p>measures until such time as implementation has been proven where this is already in place. Similarly, this same issue applies with trying to implement oversight throughout a service provider chain. Whilst in some cases this is possible, in others it is not going to be practical or achievable to cascade responsibilities down the service provider chain.</p> <p>Similarly, in relation to concentration risk, BILTIR notes that certain providers are of such a nature that there is natural concentration risk and being able to exit the relationship or have an alternative in place for back-up is not going to be possible.</p> <p>Objectives 2.4 to 2.8 touch on risk areas that may or may not directly form part of 'operational resilience' depending on each regulator's scope. These areas are always pillars of resilience, but are often regulated in separate papers/guidelines, which can create grey areas of ownership or integration.</p> | <p>Noted. Sections 2.4 to 2.8 are key elements to ensure sound approach to operational resilience and are consistent with other sectors operational resilience guidance (eg BCBS Principles for Operational Resilience). No edits made.</p> |
| General comments on Section 5 | | | |
| 62 | Bermuda International Long-Term Insurers and Reinsurers (BILTIR) | BILTIR is supportive of the objectives under section 5 as drafted with no comments. | No edits made. |
| 63 | Global Federation of Insurance Associations (GFIA) | <p>Consideration could be given for supervisors to think about how to better engage systemic or highly concentrated suppliers/third parties when it comes to operational resilience. For example, in the UK, the "CTP Oversight Regime" was created in 2024 where critical third parties are brought under the supervisory powers of the PRA/FCA/BoE instead of having financial institutions shoulder the burden alone. Consideration could also be given for supervisors to organise benchmarking of typical critical services and impact tolerances to foster industry consistency.</p> | <p>No edits made: These suggestions will be considered when finalising the Application Paper and may inform future IAIS workstreams focused on third-party risk management and operational resilience.</p> <p>In line with the Holistic Framework for Systemic Risk and the Draft application paper, we supports further exploration of supervisory approaches to third-party oversight. This includes considering mechanisms for enhanced engagement with systemic service providers, potentially through collaborative supervisory arrangements or jurisdiction-specific oversight regimes. We also agrees that benchmarking critical services and impact tolerances could contribute to greater consistency and comparability across jurisdictions. This aligns with the guidance provided under Objective 1 of the Draft Application Paper, which encourages supervisors to promote</p> |

| | | | |
|---|---|---|--|
| | | | common understanding and practices in setting impact tolerances for critical services. |
| Comments on Objective 3.1 and toolkit material | | | |
| 64 | Global Federation of Insurance Associations (GFIA) | GFIA strongly supports the emphasis on coordination between regulators to avoid siloed approaches and unnecessary duplication. A more joined-up approach across regulatory bodies is essential to ensure clarity, reduce inefficiencies, and mitigate the risk of unintended harm. Fragmented regulatory approaches can lead to confusion for firms, conflicting guidance, and increased compliance costs without necessarily improving resilience outcomes. GFIA encourages continued efforts to foster collaboration and alignment across jurisdictions and supervisory authorities. | <p>No edits made.</p> <p>We remain committed to fostering supervisory convergence and alignment through Multilateral Memorandum of Understanding (MMoU), Supervisory Forum, and ongoing work under ComFrame. These initiatives are designed to support cross-border cooperation, information sharing, and consistent application of supervisory standards. The feedback will be taken into account when we finalise the toolkit, and as we advance broader strategic priorities in support of global supervisory coordination.</p> |
| 65 | National Association of Insurance Commissioners (USA) | <p>Pg. 32, para 61, last sentence: This paragraph and section is on internal coordination and operations of the supervisor, so it seems rather odd for the last sentence to suggest external stakeholder be involved. Suggest deleting or otherwise rewording if a different point was intended. Alternatively, this may be a point better suited under Objective 3.3.</p> <p>Pg. 33, Box 16: Consider whether links for these examples should be included as their helpfulness is rather limited.</p> <p>Pg. 33, Box 16: Consider referencing the NAIC's use of "Supervisory Colleges" to support international group-level communication.</p> | <p>Pg.32, Para 61: No edits made.</p> <p>Pg. 33, Box 16: No edits made.</p> <p>Page 33 Box 16: Edits: This approach aligns with the principles outlined in ComFrame, particularly under CF 25.7, which encourages the use of Supervisory Colleges to coordinate supervisory activities and share relevant information among involved authorities. Example added from South Africa on the role of supervisory colleges.</p> |
| Comments on Objective 3.2 and toolkit material | | | |
| 66 | Global Federation of Insurance Associations (GFIA) | GFIA supports the objectives of supervisors, when appropriate, to share information and cooperate with other supervisors to minimise risk. GFIA strongly emphasises the importance of aligning operational resilience standards across global regulators and enhancing information-sharing protocols and cross-border cooperation. 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 | No edits made. We fully agree that cross-border collaboration is essential to effective supervision, particularly in the context of operational resilience, where risks often transcend national boundaries. We will consider the recommendation particularly in relation to enhancing cross-border cooperation mechanisms and promoting alignment of resilience standards across jurisdictions. |

| | | | |
|---|---|---|--|
| | | 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. | |
| 67 | National Association of Insurance Commissioners (USA) | <p>Pg. 34, para 66: Was more established stakeholder communication channels in more developed markets something demonstrated in the survey results? If so, this should be noted, otherwise this seems like a generalization that may or may not be accurate and therefore there paragraph should be deleted.</p> <p>Pg. 34, Box 17: For the USA example, provide the following links: Financial Condition (E) Committee: https://content.naic.org/committees/e/financial-condition-cmte Innovation, Cybersecurity, and Technology (H) Committee: https://content.naic.org/committees/h/innovation-cybersecurity-technology-cmte</p> | <p>Pg.34, Para 66: Deleted.</p> <p>Pg. 34, Box 17: updated the links on the document.</p> |
| Comments on Objective 3.3 and toolkit material | | | |
| 68 | Global Federation of Insurance Associations (GFIA) | GFIA supports the objective for supervisors to cooperate and communicate transparently with stakeholders. It is very important to have enhanced supervisory engagement and collaboration, including an ongoing dialogue and partnership between regulators and insurers to discuss emerging threats and best practices, to update each other and ensure both parties are aligned in expectations/understandings. | <p>No edits made.</p> <p>We agree that fostering ongoing dialogue between supervisors and the insurance industry is essential to promoting mutual understanding, identifying emerging risks, and sharing best practices. ICP 2 emphasizes transparency, accountability, and consultation in supervisory processes. We remain committed to supporting initiatives that promote open communication channels, collaborative problem-solving, and shared learning across the supervisory community and the insurance sector.</p> |

| | | | |
|---|---|--|---|
| 69 | National Association of Insurance Commissioners (USA) | Pg. 35-37, Boxes 18, 19, and 20: Consider whether links (if available) for these examples should be included. | Pg. 35 – 37 , Box 18 – 20: links will be added. |
| Comments on Objective 3.4 and toolkit material | | | |
| 70 | Global Federation of Insurance Associations (GFIA) | GFIA supports the objective for supervisors to promote a culture of continuous learning and improvement with respect to operational resilience within the supervisory authority. GFIA agrees that the areas of operational risk and information systems require a high level of technical expertise, and therefore not only insurance companies but also supervisors need to hire specialised technical staff and develop analytical tools and information management systems to enhance data analysis capabilities. | <p>No edits made.</p> <p>We welcome the GFIA’s support for the objective of promoting a culture of continuous learning and improvement in operational resilience within supervisory authorities. Also acknowledge the recognition of the technical complexity inherent in the domains of operational risk and information systems. This is consistent with Objective 3 of the <i>Draft Application Paper on Operational Resilience Objectives and Toolkit</i>, which emphasizes the importance of building supervisory capacity to assess and promote operational resilience. In addition we agree with the observation relating to development of analytical tools and robust information management systems is essential to enhancing data analysis capabilities. This aligns with the principles set out in Insurance Core Principle (ICP) 9 – Supervisory Review and Reporting.</p> |
| 71 | General Insurance Association of Japan | We agree that the areas of operational risk and information systems require a high level of technical expertise, and therefore not only insurance companies but also supervisors need to hire specialized technical staff and develop analytical tools and information management systems to improve data analysis capabilities. | <p>No edits made.</p> <p>The above comment applies.</p> |