INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

Public

Compiled Comments on Consultation on the *Draft Application Paper on Supervision of Insurer Cybersecurity* with resolutions[1]

29-June-18 to 13-Aug-2018

[1] Paragraph numbers referred in this table corresponds to the ones of the draft Application Paper on Supervision of Insurer Cybersecurity published for public consultation on 29 June 2018.

Organisation	Jurisdiction	Confidential	Answer	Proposed resolution
Q1 General comments on the Application Paper				
1. Association of Bermuda Insurers and Reinsurers	Bermuda	No	The Association of Bermuda Insurers and Reinsurers ("ABIR") represents the public policy interests of Bermuda's international insurers and reinsurers that protect consumers around the world. ABIR kindly thanks the International Association of Insurance Supervisors ("IAIS") for the opportunity to comment on the Draft Application Paper on Supervision of Insurer Cybersecurity and looks forward to being involved in the consultative process as the IAIS evaluates cybersecurity and the associated cyber risks. Overall, ABIR acknowledges the IAIS's efforts to highlight the importance of cyber resilience, recognize the appropriateness of a proportional approach to supervision and consider the benefits of regulatory convergence.	The IAIS appreciates the input from ABIR and welcomes future interaction with ABIR. Noted.
2. Insurance Bureau of Canada	Canada	No	Introduction: Insurance Bureau of Canada (IBC) is the national industry association representing Canada's private home, auto and business insurers. Its member companies represent 90% of the Canadian property and casualty (P&C) insurance market by premium volume. As a member of the Global Federation of Insurance Associations (GFIA), IBC contributed to and endorsed GFIA's submission on the International Association of Insurance Supervisors' (IAIS) Draft Application Paper on Supervision of Insurer Cybersecurity. This additional commentary reflects recent discussions with insurers operating in Canada about the IAIS' application paper. Commentary: The draft application paper is a comprehensive guide on best practices for cybersecurity in the insurance industry. Linking the G7 Fundamental Elements of Cyber Security for the Financial Sector with the Insurance Core Principles provides important guidance to supervisors and insurers on cyber risk management. As the IAIS finalizes the application paper and domestic supervisors begin considering how to implement the supervisor recommendations on the eight fundamental elements, IBC advises taking the following under consideration.	The IAIS appreciates the input from IBC and welcomes future interaction with IBC. Please see responses to GFIA's comments (Comment 3). IAIS concurs that the guidance in the Application Paper is generally principles based and is offered by the IAIS against the backdrop

			All regulation, including cybersecurity standards should be principles-based, meaning focused on outcomes. Regulation should also be targeted, practical and proportionate to the nature, scale and complexity of the measured risks, and the cost of any regulatory initiative should always be weighed against the benefits. The draft application paper recognizes the benefits of a principles-based and proportionate approach, even stating that "there is no one-size-fits-all prescription for insurers or for supervisors", that "supervisors need to tailor certain supervisory requirements and actions in accordance with the nature, size, complexity, risk profile, and culture of individual insurers", and that "recognizing the continuously evolving nature of the threat, as well as the potential benefits of regulatory convergence, this paper is generally principles-based". In Canada, as in most countries, there are insurers of various sizes, ranging from small and medium-sized enterprises to multinational corporations. The cyber threat facing an individual insurer and any associated risk to the entire financial system vary significantly. For this reason and because of the changing nature of cyber threats, a principles-based and proportionate regulatory approach is preferable. The insurance supervisors should have consistent supervisory approaches with other supervisors responsible for data and personal information protection. In Canada, the federal financial sector solvency supervisor has a cybersecurity self-assessment guidance (developed in 2013) to help insurers ensure that their cyber risk management policies and practices are appropriate and effective, the provincial insurance supervisors assess insurers' policies and procedures for protecting personal information, and the federal and provincial privacy commissioners are responsible for administering the various data and personal information protection laws. As the federal and provincial insurance supervisors enhance their focus on insurer cybersecurity practices, they should ensure that their expectations of insurers align and are consistent with the national and provincial data and personal information protection laws and privacy commissioner expectations. Recommendation: IBC recommends that prior to implementing the draft application paper's cybersecurity recommendations in Canada, the federal and provincial insurance	principles of risk-based and proportionate application. In some instances the interest in expanding the use of “best practices” suggests utility in addressing some details beyond principles. It is acknowledged that in the area of cybersecurity best approaches will evolve. Noted. The IAIS believes that any additional comment on this recommendation from the IBC is

			supervisors consult with the insurance industry to ensure that they apply them in a principles-based and proportionate manner, and consistently across the country.	rightly a matter for Canadian supervisory authorities.
3. Global Federation of Insurance Associations	Global	No	The Global Federation of Insurance Associations (GFIA) is a non-profit association established to represent national and regional insurance associations that serve the general interests of life, health, general insurance and reinsurance companies. GFIA is uniquely positioned to provide the International Association of Insurance Supervisors (IAIS) with a global perspective of global cyber risk. GFIA recognises that countries have different approaches and cultural viewpoints for addressing privacy and cybersecurity risks; however, to the extent possible, harmonisation and coordination among international governing bodies is important. GFIA's Cyber Risks working group would welcome the opportunity to have a thorough, ongoing dialogue with the IAIS on cyber risks. GFIA's global reach promotes a broad awareness of the cyber landscape and its implications for standard setters. Limiting cyber intrusions and their consequences is a shared goal of the public and private sector, and through future collaboration, GFIA believes it can help foster resilience and avoid potential unintended consequences from regulatory and standard-setting frameworks. Overall, the draft application paper is a thorough review of existing supervisory approaches to cybersecurity. Importantly, it identifies and promotes the concepts of proportionality and risk-based assessments. GFIA appreciates the effort and expertise that IAIS members and secretariat staff have put into this paper as well as the acknowledgement that there is no one-size-fits-all prescription for insurers or for supervisors. However, GFIA strongly urges caution against introducing potentially restrictive measures that may rapidly become obsolete and possibly introduce vulnerabilities due to an inflexible approach that would prevent insurers and supervisors from reacting to a rapidly changing cyber threat landscape. In particular, GFIA suggests it is inappropriate to regulate through or by prescribing/proscribing particular technologies. Technology development is fast moving and what is appropriate/inappropriate today may be obsolete tomorrow. More outcomes-focussed guidance would be appropriate as a result. GFIA respectfully recommends that the elements of proportionality and risk-based	The IAIS appreciates the input from GFIA and welcomes future interaction with GFIA The paper offers a supervisory toolkit aimed at facilitating proactive supervision of insurer cyber security. As an Application Paper it does not state any requirements. Supervisors are encouraged to consider applying proposed supervisory practices as needed and relevant, considering – among other things – the individual situation and characteristics of an insurer and the market in which it operates. The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Including this reminder at the beginning of each of the 8 sets of recommendations is a helpful suggestion, which has been

			approaches be more prominently reflected in the text, particularly before every list of specific measures outlined in the application paper. GFIA is of the view that this approach would reflect the IAIS's intent, but it should be made abundantly clear that every measure in the paper is an example and not a recommended prescriptive mandate. The sections GFIA has specifically identified are examples, and GFIA would encourage you to consider this approach in every section. GFIA would also raise the issue of consistency. Use of digital technology connects to many different aspects of insurers' businesses and how the insurance business is regulated. It is therefore understandable that different IAIS working groups and/or task forces are drafting cyber/digital related standards covering different vulnerabilities the use of digital technology could create. However, this also introduces the real risk of inconsistent drafting of guidance, and highlights the importance of coordination to avoid, for example, cyber security guidance contradicting market conduct guidance (and vice versa), which cannot be over-emphasised.	adopted. Please see response to Comment 10. This concern is noted and the IAIS has in place practices to minimize the risks described by GFIA.
4. Institute of International Finance	Global	No	The Institute of International Finance and its members ("IIF") appreciate the International Association of Insurance Supervisors (IAIS)' efforts dedicated to the important issue of cybersecurity, and we welcome the opportunity to provide input to the Draft Application Paper on Supervision of Insurer Cybersecurity. The IIF has been actively engaged in digital technology and cybersecurity-related discussions and is committed to constructive dialogue with standard setting bodies including the IAIS and FSB. In general, we are fully supportive of the IAIS' undertaking in cybersecurity, cyber risk management and cyber resilience issues. We believe it is important for the public and private sector to cooperate on tackling the evolving threat and risk landscape as laid-out in this paper or as they continuously evolve with new technologies. We stand ready to provide input to the IAIS on the development of this topic going forward. As a follow-up development to the 2016 IAIS Issues Paper on Cyber Risk to the Insurance Sector that focused on describing the cyber risk landscape and its threat to the insurance sector, this Application Paper provides a good overview of current cybersecurity standards and guidance. While we understand that the purpose of Application Papers is to provide additional material instead of establishing standards, the frequent use of "should" throughout the Application Paper goes beyond guidance. As a general principle, we would urge the IAIS to be cautious in	The IAIS appreciates the input from IIF and welcomes future interaction with IIF. “Should” is commonly used across IAIS materials as an indication of guidance – not a requirement. Its use in the Application Paper does not imply a requirement or a standard, but a good practice. The Application Paper will reflect that as

			presenting the guidance in Application Papers, and to keep considerations open and flexible when taking any potential next steps on the recommendations. As referenced in the IAIS Application Paper, the work of the Financial Stability Board (FSB) on a cyber lexicon will, and should, strongly influence the IAIS work on insurer cybersecurity. In parallel to the IIF Insurance Working Group (IWG) which oversees the response to this Application Paper, the IIF formed a cross-sectoral Cybersecurity Working Group (CWG), consisting of global banks and insurers as a platform for discussions that promote a comprehensive understanding of the issue across financial sectors. In support of this goal, the CWG together with interested members of the IWG is working on a response to the FSB public consultation on the cyber lexicon. As a general message from both working groups, we welcome the FSB objective of developing a cyber lexicon - "a cross-sector common understanding of relevant cyber security and cyber resilience terminology, the assessment and monitoring of financial stability risk of cyber risk scenarios, information sharing as appropriate and the elaboration of guidance related to cyber security and cyber resilience, including identifying effective practices." In our review, we have noted important differences between the definitions of key concepts, such as "cyber risk" and "cybersecurity", in the proposed FSB Cyber Lexicon and this Application Paper, and we would like to request more collaboration and consistency between the FSB and the IAIS on the development of this topic going forward. Key issues policymakers should consider when evaluating the current policy framework for these rapidly developing issues are the inefficiencies of compliance with overlapping standards, as well as the cost of regulatory and legal fragmentation, which should be addressed and avoided. These issues were developed more extensively in the IIF Staff Paper: Addressing Regulatory Fragmentation to Support a Cyber-Resilient Global Financial Service Industry .The digital area encompasses many different aspects of insurers' business and how it is regulated. It is therefore understandable that different IAIS working groups and/or task forces may be required to focus on the different aspects of the use of digital technology. However, this also introduces the real risk of drafting inconsistent guidance and highlights the importance of coordination to avoid contradictory cyber	with all IAIS supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. The IAIS has participated in the FSB cyber lexicon project and is supportive of its goals. Although the FSB cyber lexicon will not be published in time to serve as a definitive resource for this Application Paper, the IAIS expects that the cyber lexicon will inform future relevant work. Please see response to Comment 3.

			security guidance; for example, market conduct guidance (and vice versa) cannot be over-emphasized. Therefore, we would like to highlight the importance of coordination among different policymakers, regulators and supervisors when addressing cyber risks and cyber security. In addition, we believe that any cybersecurity legislation should be principles-based and consist of outcomes-focused guidance with a view to accomplishing agreed objectives. In our view, legislative practice to regulate through or prescribe/proscribe particular technologies should be avoided. Technological developments are fast moving and what is appropriate or inappropriate today may be obsolete tomorrow. For example, encryption is a common means of securing data today. Tomorrow, encryption could be superseded by a new or different way of protecting data. We also believe that a risk-based approach should be taken in the guidance provided. Depending on the insurer, the large number of stakeholders, and third-party service providers involved in its operations and transactions do not all pose the same level of (cyber) risk. We therefore urge the IAIS to take a risk-based approach when providing guidance or recommendations for cybersecurity frameworks, strategies and risk management practices.	Please see response to Comment 2. Please see above as well as responses to Comments 2 and 3.
5. AIA Group	Hong Kong	No	AIA is pleased to provide comments on the draft application paper on Supervision of Insurer Cybersecurity. AIA strongly supports the development and promotion of effective and proportionate regulatory and supervisory measures on cybersecurity. AIA also appreciates that the IAIS has drafted an application paper for supervisors to help with the practical application of the principles-based requirements of the Insurance Core Principles. We agree that supervisory measures should not go beyond what is necessary. One of our key comments on the draft application paper is that while we agree with the objectives of the risk and control assessment, the requirements under paragraph 103 are extensive and prescriptive. In particular, it is not practical for all assets and that the classification and inventory related controls be focused primarily on critical assets for sub-paragraphs c, d, e. We understand that this draft application paper is work-in-progress and look forward to the compiled comments on the consultation and participating in any further consultations or discussions.	The IAIS appreciates the input from AIA and welcomes future interaction with AIA. Please see response to Comment 51.

6. The Geneva Association	International	No	We would like to thank the IAIS for providing us with the opportunity to comment on the draft Application Paper on Supervision of Insurer Cyber Security. We are aware that the Institute of International Finance (IIF) is also going to respond to this draft Application Paper and we are familiar with their upcoming response. We would like to express our support for and alignment with the IIF response. We appreciate that the draft Application Paper is a follow-up on the Issues Paper on Cyber Risk to the Insurance Sector which was launched in April 2016. The Geneva Association, when asked to suggest topics to be taken on board in the IAIS next Strategic Plan, suggested to consider topics such as cyber risk as well as the development of a cyber insurance market. The 2016 issues paper put supervision of insurer cyber risk on the policy agenda and raised awareness for both the supervisory community and insurers as to which challenges cyber risk could pose to the industry. With the recent draft Application Paper, the IAIS Financial Crime Task Force has done well in taking the issues further by providing practical guidance to supervisors to help them address cyber risk by pointing to the existing IAIS toolkit, including Insurance Core Principles (ICPs) that could be used to address the risk. What becomes apparent from the paper is that the issue of cyber risk cannot be addressed by supervisors or insurers alone, but needs cooperation. As rightly stated in the draft, the interests of supervisors and insurers are aligned in this field. When looking at the paper from an information security point of view, there is potential to improve the draft Application Paper further. Mentioning could be made to emerging trends in the IT landscape, including the use of Internet of Things as well as cloud based services used on a large scale. Macro trends that confront the insurance industry as well as its supervisors with new risks, include: 1) cloud sprawl which could create or magnify risks to business processes and operations, not least as firms may lose control over their data and intellectual property; 2) the risk of (residual) firm data outside of controlled environment due to the rapid spread of `bring your own device' policies in firms combined with the use of cloud based platforms across devices; 3) lack of agreed on cyber risk definitions and mitigation approaches. Some of the above risks could be addressed by increased transparency and by creating a culture in which an open discussion on cyber risk and information security gaps can	The IAIS appreciates the input from the Geneva Association and welcomes future interaction with the Geneva Association. It is acknowledged that in the area of cybersecurity best approaches will evolve. The IAIS is of the view that the principles addressed in the Application Paper are responsive to these recommendations, without being overly prescriptive or focused on approaches that may become outdated. Notwithstanding the IAIS appreciates these timely

			take place in a non-punitive environment. 4) Agreed upon definitions of cyber risks, scenarios and mitigation measures would provide the industry with tools to support the adoption of a risk-based cyber approach. Lastly, there is a need for risk transfer mechanisms to help mitigate cyber and information security risks. In addition to the abovementioned points we would suggest to include a core set of IT hygiene and response measures in the paper, including response procedures with regard to certain types of incidents (such as malware, ransomware or DDoS attacks). We recognize that the draft Application Paper serves as a guidance and does not introduce new standards. We are generally positive towards the draft and hope the suggestions above can be taken into account. Beyond the suggestions above, we have submitted some comments to specific parts of the paper through the consultation tool. We would also be keen to provider further explanation to the points raised if needed The Geneva Association is strongly committed to continuing the constructive dialogue and cooperation with the IAIS and stands ready to provide additional views or clarifications. Should you have any questions on the issues raised in this letter, please contact Peter Skjoedt (peter_skjoedt@genevaassociation.org), or Dennis Noordhoek (dennis_noordhoek@genevaassociation.org).	observations and encourages continued dialogue. Please see specific responses where the comments appear. Noted with appreciation.
7. General Insurance Association of Japan	Japan	No	We, the General Insurance Association of Japan (GIAJ), believe that what the Draft Application Paper on Supervision of Insurer Cybersecurity (hereinafter referred to as "AP") describes is going in the right direction. However, against the background of cybersecurity risks not being issues particular to insurers, we think it is more appropriate to consider potential insurance-specific guidelines and rules based on comprehensive guidelines for the whole financial sector so that their integrity in relation to sector-wide guidelines and regulations is maintained and unnecessary duplication is avoided. If there are no significant or industry-specific risks, the current ICPs which already encompass the issues presented by cyber risks should be sufficient for the supervision of insurer cybersecurity. If the current ICPs are found to be insufficient, we believe it is appropriate to revise the ICPs to make up for the shortfall.	The IAIS appreciates the input from the GIAJ and welcomes future interaction with the GIAJ. Please note that the Application Paper does not offer rules. Please see response to Comment 3.

			In any case, we are still not convinced that the insurance industry needs to develop its own guidelines or rules even after taking into consideration the contents of the AP. Therefore, when developing rules particular to insurers, the IAIS should clearly express its rationale. Judging by the fact that the introductory statements in the "Recommendation" section of the AP often use the word "may", such as in paragraphs 48 and 81, we understand "Recommendations" to mean "best practices". Additionally, almost all of the sentences in the latter part of the document use the words "should" or "must", which therefore indicates a lack of balance. We believe that the words "should" and "must" should be replaced with "may" and "would" so that supervisors and insurers can exercise discretion in accordance with the materiality of the issue.	"Should" is commonly used across IAIS materials as an indication of guidance – not a requirement. Its use in the Application Paper does not imply a requirement or a standard, but a good practice. The Application Paper will reflect that as with all IAIS supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application.
8. Zurich Insurance Company Ltd.	Switzerland	No	Zurich appreciates the efforts of the IAIS in regard of cybersecurity, and we welcome the opportunity to comment the Draft Application Paper (AP) on the Supervision of Insurer Cybersecurity. As a follow-up to the 2016 Issues Paper (IS) on Cyber Risk to the Insurance Sector that focused on describing the cyber risk landscape and its threat to the insurance sector, the AP helps with the practical application of supervisory material to cyber risk, cybersecurity and cyber resilience. The IAIS however fails to recognize significant technological macro trends that affect the cyber and information security profession, today, in its mandate to defend organizations and drive cultural improvements. These macro trends require fundamental changes to cybersecurity tactics, safeguards and operating models. We have outlined a few of the risks and recommendations for your consideration. Trends and associated risks Risk 1: Cloud sprawl is creating or magnifying risks to business processes and operations. The ubiquity of cloud in the marketplace for all computing options, the diversity of management practices among providers, and the added underlying	The IAIS appreciates the input from Zurich and welcomes future interaction with Zurich. Please see responses to Comment 6. The IAIS concurs that to the degree feasible insurers, supervisors and the larger financial

			technical complexity, which support business processes and value chains, are significant. This needs to be addressed from a risk perspective, with new approaches to practically secure, manage and maintain these environments resilient. - The offers of cloud providers seldom account for security and privacy considerations that their customers e.g. insurers must add - Using multiple interlinked cloud providers creates technical complexity that makes supporting business processes across cloud environment challenging - Adding planning and governance to cloud projects significantly increases the time to adoption and increases costs, making security and privacy a cost additive proposition and incentivizing minimization of these capabilities Risk 2: Empowered end users are being asked to manage data using complex tools in an ever-increasing device landscape. Moving data between company servers, laptops, to employee owned mobile devices and any other computer becomes seamlessly possible, and the potential for residual data to exist outside of controlled environments expands exponentially. - Technology is enabling data to travel inside and outside of organizations fluidly - This situation places more responsibility on the end user to appropriately use fast changing and increasingly complex environments - Remaining up to date on technology uses "best practices' for keeping data secure and private is becoming increasing complex - New technology emphasizes end-user flexibility over defined use case, exacerbating security and privacy risks Risk 3: Organizations vary in their abilities to define cyber and information security risks, which leads to different approaches, levels of rigor and completeness. Organizations can benefit from a common set of risks, a universe of risks, or guidelines for risks to establish a common set reference to address. To date, many organizations still use compliance as the main benchmark. - Risks are defined significantly differently from organization to organization - Definition of the risks significantly impacts the investment and focus on cyber and information security, which impacts distribution of investments, people and attention - Having a common set of risks, or scenarios or guidelines on how to define risks could benefit the industry and provide common footing for programs Recommendations	services industry will need to work together to monitor and implement evolving best practices that will meet the changing risk landscape so as to protect the confidentiality, integrity, and accessibility of insurer and consumer data.

			Incentivize transparency. We encourage the IAIS and other relevant standard-setting bodies to devise a more open and transparent cybersecurity climate, so that the CISO profession can mature and focus on the risks rather than on "being compliant". Looking back ten years, many companies were hesitant to admit the potential for a security incident, breach or non-compliance. Now the pendulum has swung and security professionals speak about concepts like presumed breach, companies have "hunt teams" which specialize in finding digital intruders and CISO speak openly at conferences about the inability to defend against every threat. Newer regulations like GDPR in the EU allow for a risk-based approach that acknowledges the need to mature capabilities and close gaps over time. However, what companies are focusing on to mature, and how long improvements are expected to take to achieve full implementation are not discussed openly with confidence. Mechanisms and channels are needed to support active discussion as well as acknowledge and address cyber and information security gaps in a non-punitive atmosphere. Define an industry risk universe and risk scenarios. With the move to risk-based approach to cyber and information security gaining adoption across companies, there is a vacuum in the industry about what risks to look at or even how to define risks. Companies have varying levels of cyber risk expertise, and this leads to large discrepancies in how risks are defined, evaluated and ranked by companies. Defining a risk universe to create a baseline of what organizations should seek to defend against, or defining scenarios to test against can provide much needed guidance. Current existing frameworks and guidance from NIST, ISO and others do not take the crucial step of articulating risks. This guidance could assist with: industry comparison across companies, inputs for strategic planning and prioritization of investment, inputs for crisis management drills, and the basis for board level evaluations. Promote adoption of cyber and information security risk transfer. To allow companies to take chances, innovate and compete in the global economy, risk transfer mechanisms are needed to help mitigate cyber and information security risks. Examples include insurance and insurance linked securities that can promote a cybersecurity mindset and protect organizations from financial implications. Steps need to be taken to promote or even mandate risk transfer mechanisms or vehicles for companies.	Cyber insurance is beyond the scope of this Application Paper.

9. ACLI	United States	No	The issue of cybersecurity has been increasingly in the news media, due mostly to many high profile cyber breaches at major companies. Due to this increasing threat and its impact on consumers, insurance supervisors from around the world have also increased their focus on the issue of cybersecurity to that end the IAIS drafted an Application paper to provide guidance to insurance supervisors to help develop or enhance their approach to cyber risk. As the IAIS states in its introduction, "the nature and of cyber risk requires supervisors to exercise increase scrutiny or insurers." ACLI appreciates the IAIS focus on this issue and further their belief that all parties should decrease their cyber risks. However, ACLI has concerns with much of the proposed guidance, which can be viewed as prescriptive and rigid. We appreciate your consideration of our comments.	The IAIS appreciates the input from ACLI and welcomes future interaction with ACLI. The paper provides a supervisory toolkit aimed at facilitating proactive supervision of insurer cyber security. As an Application Paper it does not state any requirements. Supervisors are encouraged to consider applying proposed supervisory practices as needed and relevant, considering – among other things – the individual situation and characteristics of an insurer and the market in which it operates. Please see responses to specific comments.
10. American Insurance Association	United States of America	No	Overall, the Applications Paper presents a thorough review of existing supervisory frameworks. The use of existing frameworks, to the extent possible, helps promote consistency and harmonization, which are important elements of global supervisory recommendations. Additionally, in order to promote cyber resiliency, regulatory guidance must be flexible, risk-based, and proportional. These fundamental principles allow insurance licenses to adapt to the evolving threat landscape and technological innovation. Further, no company is immune from cyber risks; however, principled and risk-based regulation encourages and supports a well-balanced approach to maximizing human and capital resources while protecting systems and data. Importantly, the Introduction of the Applications Paper highlights the need for proportionality and a risk-based approach to cybersecurity supervision. Nevertheless, we believe that these important principles get lost throughout the paper and instead it takes a prescriptive approach at times. A risk-based approach	The IAIS appreciates the input from AIA and welcomes future interaction with AIA. Please see responses to Comment 3.

			to cybersecurity is the only viable method of ensuring that we are adequately protecting our insured's data. The recommendations that follow are intended to reinforce that supervisory guidance should be flexible, proportional, risk-based and principled. We note that every paragraph introducing a new set of recommendations states as follows: "With regard to insurers' cybersecurity strategy and framework, it may be appropriate for supervisory practices to encourage or reflect the following." To emphasize the principles noted above, we encourage the drafters to include an additional phrase similar to the following at the end of the sentence everywhere it appears in the document, "in a risk-based and proportional manner." Additionally, given that the Application Paper identifies a number of international frameworks that insurer's reference, we are curious as to why there are specific sections mapping the ICPs to the G7FE. It seems inconsistent to identify current supervisory examples, yet to pull out a single Framework for mapping purposes without a discussion as to whether that should, in fact, be the threshold measurement. We recommend removing the G7FE mapping sections and instead include those same observations as a specific element of the "Example of Current Practices" sections.	The IAIS has included this additional wording suggested by AIA to more clearly reflect that, as with all supervisory material, this guidance in the Application Paper is offered against the backdrop principles of risk-based and proportionate application. Also, paragraph 16 has been revised to more clearly describe the IAIS concepts of proportionality and risk-based application of supervisory materials. The G7FE is an internationally developed set of widely agreed cybersecurity principles applicable to the financial sector. The IAIS offers the mapping as a means of considering the current state of the ICPs with respect to the cybersecurity topic.
11. Cincinnati Insurance Company	United States of America	No	The IAIS wades into field of insurer cybersecurity with its "Draft Application Paper on Supervision of Insurer Cybersecurity." In submitting this Draft Application Paper for worldwide review and comment, the IAIS states that it seeks to propose "supervisory practices for the insurance sector" regarding cybersecurity. Claiming broad authority "under the Insurance Core Principles," the IAIS invites insurers to "consider this Application Paper to assist in developing and implementing good cybersecurity practices in their organisations." As we have stated many times in similar sets of consultation comments, our company does not believe that the world needs a set of Insurance Core Principles (ICPs) and objects to the program under which the International Monetary Fund (IMF) grades the U.S. insurance regulatory system on its compliance with the ICPs. The core principles upon which the U.S.	The IAIS appreciates the input from Cincinnati and welcomes future interaction with Cincinnati. The comments are beyond the scope of this consultation.

			insurance regulatory system is premised have functioned perfectly for over 150 years and do not need an overhaul by the International Association of Insurance Supervisors (IAIS) or by its ostensible parent organization, the Financial Stability Board (FSB). Therefore, we object to the IAIS promulgating this ICP-premised Draft Application Paper, and would request that the IAIS withdraw it from further consideration. There is no need for the IAIS to craft a new international insurance code on insurance cybersecurity, or to otherwise claim authority to regulate insurance cybersecurity. The U.S. and other regulatory regimes are capable of regulating insurance cybersecurity on their own without interference by the IAIS. Given the substance of this comment (the Draft Application Paper on Supervision of Insurer Cybersecurity should be withdrawn), we see no need to answer Q2 through Q280.	
12. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest an editorial review for missing periods/spacing/missing words or commas and ensure correct use of italics for consistency.	Concur.
Q2 General comments on Section 1:				
Q3 Comment on Paragraph 1				
Q4 Comment on Paragraph 2				
Q5 Comment on Paragraph 3				
Q6 Comment on Paragraph 4				
Q7 Comment on Paragraph 5				
Q8 Comment on Paragraph 6				
Q9 Comment on Paragraph 7				
Q10 Comment on Paragraph 8				
Q11 Comment on Paragraph 9				

Q12 Comment on Paragraph 10				
Q13 Comment on Paragraph 11				
Q14 Comment on Paragraph 12				
Q15 Comment on Paragraph 13				
13. American Insurance Association	United States of America	No	The definition of "cyber risk" is overly broad for the purpose of this Application Paper. We note throughout our comments that a risk-based approach to cyber is critical. The overly broad definition of "cyber risk," which attempts to include "any" event emanating from electronic data and transmissions is essentially a catch-all that does not recognize the different scenarios and potential hits on a system that are avoided and would not, and should not, give rise to concern in a risk-based approach. For this reason, we have borrowed some elements from the United States insurance regulatory community to suggest a more risk-focused definition that could read, for example: "an actual risk emanating from unauthorized access to, disruption or misuse of, an Information System or non-public information stored on such Information System that is not encrypted or otherwise rendered unreadable." AIA is also watching, and intends to comment on, the Financial Stability Board's Cyber Lexicon and highlight that some of the language evidencing an impact on confidentiality, integrity, and availability of the Information System may be additional risk-based language that the IAIS may want to consider.	The IAIS has participated in the FSB cyber lexicon project and is supportive of its goals. Although the FSB cyber lexicon will not be published in time to serve as a definitive resource for this Application Paper, the IAIS expects that the cyber lexicon will inform future relevant work.
Q16 Comment on Paragraph 14				
Q17 Comment on Paragraph 15				
Q18 Comment on Paragraph 16				
14. Association of Bermuda Insurers and Reinsurers	Bermuda	No	ABIR supports the paper's recognition of the appropriateness of supervisors considering proportionality in the application of supervision in this area. We encourage the IAIS to ensure that this message is prominent in the final draft to enable supervisors to tailor their supervision in this area commensurate with the risks based on the individual entity or group.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.

15. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Third sentence, remove "while".	No revision necessary.
Q19 Comment on Paragraph 17				
16. AIA Group	Hong Kong	No	Similarly, for the reasons that the nature, size, complexity and risk profile of the insurer as well as the jurisdiction in which it operates in should be taken into consideration in implementing any supervisory measures, we agree that such supervisory measures on cybersecurity should not by nature be prescriptive.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
Q20 Comment on Paragraph 18				
Q21 Comment on Paragraph 19				
Q22 General comments on Section 2:				
Q23 Comment on Paragraph 20				
Q24 Comment on Paragraph 21				
Q25 Comment on Paragraph 22				
Q26 Comment on Paragraph 23				
Q27 Comment on Paragraph 24				
Q28 Comment on Paragraph 25				
Q29 Comment on Paragraph 26				
Q30 Comment on Paragraph 27				

Q31 Comment on Paragraph 28
Q32 Comment on Paragraph 29
Q33 Comment on Paragraph 30
Q34 Comment on Paragraph 31
Q35 Comment on Paragraph 32
Q36 Comment on Paragraph 33
Q37 Comment on Paragraph 34
Q38 Comment on Paragraph 35
Q39 Comment on Paragraph 36
Q40 Comment on Paragraph 37
Q41 Comment on Paragraph 38
Q42 General comments on Section 3:
Q43 Comment on Paragraph 39
Q44 Comment on Paragraph 40
Q45 Comment on Paragraph 41
Q46 Comment on Paragraph 42
Q47 Comment on Paragraph 43
Q48 Comment on Paragraph 44
Q49 Comment on Paragraph 45
Q50 Comment on Paragraph 46

17. Institute of International Finance	Global	No	We would propose a slight change of wording in this paragraph by replacing the word "ratified" with "overseen" in order to more accurately account for the role of the Board in developing or adopting a corporate cybersecurity strategy.	The Application Paper has been revised in several places in response to suggestions to better reflect the roles of the board and management, consistent with the ICPs. Please see response to Comment 40 and 43. “Ratified” replaced by “overseen” as suggested by IIF. The IAIS believes the language in this paragraph reflects the importance of board level attention to that issue.
18. The Geneva Association	International	No	ICP 8 addresses "risk management and control." Consistent with ICP 8.1 and supporting guidance regarding developing suitable risk management strategies and processes, insurance supervisors should encourage every insurer to develop or adopt a cybersecurity strategy and framework and have such strategy and framework (strike `ratified' replace with `overseen' by its Board. GA comment: We would propose a slight change of wording in this para by replacing the word "ratified" with "overseen" in order to more accurately account for the role of the Board in developing or adopting a corporate cybersecurity strategy.	Please see response to Comment 17.
19. ACLI	United States	No	A company´s Board is tasked with overseeing an entire corporation, while day to day operations are undertaken by a company’s senior management. We therefore request this paragraph be rewritten to say: "ICP 8 addresses "risk management and control." Consistent with ICP 8.1 and supporting guidance regarding developing suitable risk management strategies and processes, insurance supervisors should encourage every insurer to develop or adopt a cybersecurity strategy and framework and have such strategy and framework overseen by its Board."	Please see response to Comment 17.
20. American Insurance Association	United States of America	No	This paragraph should be amended to more accurately reflect the role of the Board in the risk management structure as one of oversight and to highlight the need for risk-based cybersecurity programs. As such, we recommend the following	Please see response to Comment 17.

			amendments: "Consistent with ICP 8.1 and supporting guidance regarding developing suitable risk management strategies and processes, insurance supervisors should encourage every insurer to develop or adopt a RISK-BASED cybersecurity strategy and framework and have such strategy and framework OVERSEEN by its Board." Our proposed language is highlighted in caps above and we deleted "ratified."	
Q51 Comment on Paragraph 47				
Q52 Comment on Paragraph 48				
21. Association of Bermuda Insurers and Reinsurers	Bermuda	No	In principle, ABIR supports the recommendations for supervisors regarding cybersecurity strategies and cybersecurity frameworks listed in paragraph 48, (a) - (h), however we respectfully suggest that the IAIS consider the inclusion of language that reinforces the proportionality principle to ensure the supervisors expectations are commensurate with the risk profile of the entity or group.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
22. Global Federation of Insurance Associations	Global	No	GFIA supports the intent behind the concepts and considerations outlined in Paragraph 48, but would recommend preserving the concept of proportionality and risk-based assessment by changing "should" to "may" in subparagraphs a through h. Alternatively, a sentence could be added to identify that the manner in which each recommendation is implemented will depend on individual risk and proportionality calculations. Unfortunately, the nature of the risk dictates that no entity, private or public, can be entirely secure. An entity can be expected to take only all "reasonable" measures to limit cyber intrusions and address their consequences. To that end, GFIA recommends the following amendment: "Therefore, framework objectives should aim to maintain and promote the insurer's ability to reasonably anticipate, detect, withstand, contain, and recover from cybersecurity incidents".	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10. The IAIS has retained the original language, but has modified the introductory paragraph as described in response to Comment 10.
23. Institute of International Finance	Global	No	Depending on the insurer, it may have hundreds of stakeholders, other insurers, and third party service providers. They do not all pose the same level of (cyber) risk. We would therefore urge that a risk-based approach be weaved into this guidance.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based

				and proportionate application. Please see response to Comment 10.
24. The Geneva Association	International	No	G52 g) (add `Based on risk'), an insurer's cybersecurity framework should consider how the insurer would regularly review and actively mitigate the cyber risks that it bears from and poses to its stakeholders such as policyholders, other insurers, third party service providers (including the services and products provided by those third party service providers), and other third parties (the insurer's cybersecurity ecosystem). GA comment: depending on the insurer, it may have hundreds of stakeholders, policyholders, other insurers, and third party service providers. They do not all pose the same level of (cyber) risk. We would therefore urge that a risk-based approach be weaved into this guidance.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
25. General Insurance Association of Japan	Japan	No	Comment on 48.d. It is the responsibility of the insurer's Board to appropriately define the respective roles and responsibilities of itself and its management so that its cybersecurity framework is effective. Therefore, the insurers' discretion should be allowed on this point.	The IAIS is of the view that paragraph 48(d) is not in derogation of the point made by GIAJ. Please see response to Comment 10.
26. ACLI	United States	No	ACLI agrees with the intent many of the IAIS proposed changes, however, it appears its specific recommendations are overly prescriptive or simply just too broad. On a general level, under paragraph 48 and its subparagraph, the IAIS may consider changing its references to what an insurer "should" do to instead what an insurer "may" do. Insurers range in sizes and the IAIS should ensure that any guidance to supervisors is risk-based and empowers the insurer to institute the cyber protections most relevant to the threats they face. Under paragraph 48(b), the IAIS outlines what an insurer's cybersecurity framework should support and promote. ACLI would request the inclusion of the term "reasonably" into the second full paragraph so it would read "Therefore, framework objectives should aim to maintain and promote the insurer's ability to reasonably anticipate, detect, withstand…"	The paper provides a supervisory toolkit aimed at facilitating proactive supervision of insurer cyber security. As an Application Paper it does not state any requirements. Supervisors are encouraged to consider applying proposed supervisory practices as needed and relevant, considering – among other things – the individual situation and characteristics of an insurer and the market in which it operates.

			Under paragraph 48 (g), we request the inclusion of the following term at the beginning of the paragraph: "To the extent feasible and based on risk..."	Please see response to Comments 10 and 22.
27. American Insurance Association	United States of America	No	Consistent with our recommendation to promote proportional, flexible and risk-based approaches to cybersecurity throughout the paper, we suggest, subparagraph (g) should be amended to begin with "TO THE EXTENT FEASIBLE AND BASED ON RISK, an insurer …" Our proposed language is highlighted in caps above.	Please see response to Comment 10.
28. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest changing the introductory paragraph sentence as follows: "With regard to insurers' cybersecurity strategy and framework, supervisory practices may encourage or reflect the following, where appropriate". Change first sentence in e) to "insurer should align its cybersecurity framework…" as this would make it consistent with other sections.	Please see response to Comment 10. Concur and revised accordingly.
Q53 Comment on Paragraph 49				
29. Association of Bermuda Insurers and Reinsurers	Bermuda	No	ABIR acknowledges that there are potential benefits of regulatory convergence. Paragraphs 49 - 69, describe various jurisdictions' approaches to the regulation and supervision of cybersecurity, highlighting the potential challenge with achieving regulator convergence. We recommend that in the finalization of the application paper the IAIS ensure that in general the guidance provided maintains a non-prescriptive and proportional approach so as not to add additional complexities for the supervision of global insurance groups.	Noted and concur. Please see responses to Comments 3, 4, and 10.
Q54 Comment on Paragraph 50				
Q55 Comment on Paragraph 51				
Q56 Comment on Paragraph 52				
Q57 Comment on Paragraph 53				
Q58 Comment on Paragraph 54				
Q59 Comment on Paragraph 55				

Q60 Comment on Paragraph 56				
Q61 Comment on Paragraph 57				
Q62 Comment on Paragraph 58				
Q63 Comment on Paragraph 59				
Q64 Comment on Paragraph 60				
Q65 Comment on Paragraph 61				
Q66 Comment on Paragraph 62				
Q67 Comment on Paragraph 63				
Q68 Comment on Paragraph 64				
30. American Insurance Association	United States of America	No	It is true that the NAIC Insurance Data Security Model Law outlines expectations related to notification of a breach, but primarily these are related to notice to the insurance regulator and not to the consumer. Insurance licensees are still obligated to comply with the patchwork of state consumer breach notification requirements. Also, we recognize that paragraph 65 clarifies that the Model Law is not effective unless adopted by the states, nevertheless, we believe this point should also be mentioned in paragraph 64 to be abundantly clear as to the role of the NAIC Model Law. Paragraph 64 may be amended to read: The National Association of Insurance Commissioners (NAIC) adopted the Insurance Data Security Model Law in 2017, creating RISK-BASED rules for insurers, agents, and other licensed entities covering data security, investigation, and SUPERVISORY notification of breach. AS NOTED BELOW, THE MODEL SERVES AS A ROADMAP FOR INDIVIDUAL STATE REGULATION, BUT IS NOT EFFECTIVE IN A STATE UNLESS ADOPTED AS LAW IN THAT STATE. This includes maintaining an information security program based on on-going risk assessment, overseeing third party service providers BASED ON RISK, investigating data breaches and notifying regulators of a "cybersecurity event."	No change necessary, The IAIS notes the NAIC description of its model.

			Our proposed language is highlighted in caps above.	
31. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest including the following (either in the paragraph or as a footnote): "South Carolina is the first U.S. state to enact the NAIC Insurance Data Security Model Law, which will become effective on 1 January, 2019."	The IAIS has inserted the NAIC's revision to this paragraph.
Q69 Comment on Paragraph 65				
32. Institute of International Finance	Global	No	We would like to note that the Model laws do not create rules. We suggest rewording this to reflect the fact that model laws provide guidance for state legislatures to consider in drafting legislation for possible adoption into state law as described in Para 65.	Please see response to Comment 30.
Q70 Comment on Paragraph 66				
Q71 Comment on Paragraph 67				
Q72 Comment on Paragraph 68				
Q73 Comment on Paragraph 69				
Q74 Comment on Paragraph 70				
Q75 Comment on Paragraph 71				
Q76 Comment on Paragraph 72				
Q77 Comment on Paragraph 73				
Q78 Comment on Paragraph 74				
Q79 Comment on Paragraph 75				
33. Institute of International Finance	Global	No	We have some concern that this paragraph does not properly capture the responsibilities of Boards versus Senior Management. We would therefore request	This paragraph and others have been revised in response to suggestions to better reflect the

			that "and" in the second sentence be changed to "or". (...,boards or senior management can...)	roles of the board and management, consistent with the ICPs. Please see responses to Comments 17, 40, and 43.
34. The Geneva Association	International	No	Active senior management or board-level engagement implies oversight of the design, implementation and effectiveness of cybersecurity programmes. Informed by information on threats and vulnerabilities and their entity's risk appetite, boards (delete `and' replace with `or') senior management can drive risk-management decisions, oversight and accountability in both the short- and long-term. As such, boards and senior management can use decision-making to drive cybersecurity programmes beyond the traditional views of compliance. GA Comment: we have some concern that this para does not properly capture the responsibilities of Boards versus senior management. We would therefore request that the use of the word "and" in the second para be changed to "or" as edited above.	Please see response to Comment 33.
35. ACLI	United States	No	We recommend altering this paragraph to include the term "or" in lieu of "and" when determining risk-management decisions. Companies differ in their governance, and the IAIS should ensure to foster the differences among companies.	Please see response to Comment 33.
36. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest rephrasing the last sentence for clarity.	Please see response to Comment 33.
Q80 Comment on Paragraph 76				
Q81 Comment on Paragraph 77				
Q82 Comment on Paragraph 78				
Q83 Comment on Paragraph 79				

Q84 Comment on Paragraph 80				
Q85 Comment on Paragraph 81				
37. Association of Bermuda Insurers and Reinsurers	Bermuda	No	With respect to the paper's recommendations for supervisors regarding governance, the guidance indicates that "each insurer should designate a senior executive, such as a Chief Information Security Officer (CISO), to be responsible and accountable overall for the cybersecurity framework…". ABIR wishes to point out that this language appears to be prescriptive and not aligned with the proportionality principle that is believed to be the intent of the IAIS in this area. ABIR recommends that language in this area be amended to include the designation of an individual with adequate skills, who is appropriately positioned within the organization, to be responsible and accountable for the cybersecurity framework based on the size and the complexity of the organization.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10. Paragraph 81 has been revised for clarity.
38. Global Federation of Insurance Associations	Global	No	Respectfully, GFIA recommends aligning this section with the guidance's intent to have a risk-based and non-prescriptive approach. The Board certainly has an important role in cybersecurity oversight, but GFIA is concerned that this section may miscategorise the Board's role in some instances. For instance, where there is a recommendation for the Board "and" senior management to perform a task, "or" may be a more appropriate word choice. There is an opportunity for the application paper to clarify and distinguish between the Board and senior management. The Board must be aware of the risks and framework to manage enterprise-wide cyber risk, but senior management should establish the methodology for implementing that framework. Similarly, in paragraph 81, subparagraph f there is a recommendation that "each insurer should designate a senior executive, such as a Chief Information Security Officer (CISO)". Requiring all insurers to have a CISO or similar position may not be possible or appropriate given the needs and resources of some insurance groups. Rather than recommending a CISO, GFIA encourages the IAIS to consider a recommendation that an employee, affiliate, or outside vendor should be responsible for implementation of the organisation's overall cybersecurity framework.	Please see responses to Comment 17 and 40. Please see response to Comment 37.
39. Institute of International Finance	Global	No	Sections 81 a) and b) both overweight the role of, and assign too much responsibility to, the Board. In both instances, Senior Management will necessarily be involved in decisions around setting the firm's tolerance for cyber risk as well as	Please see responses to Comments 17 and 40.

			considerations around changes to products, services, policies or practices in light of the company's cyber risk profile.	
40. The Geneva Association	International	No	Q81a: The insurer's Board should be ultimately responsible for setting strategy and ensuring that cyber risk is effectively managed. The Board, (add `in conjunction with senior management') , should (add `oversee' remove `endorse') the insurer's cybersecurity framework and set the insurer's tolerance for cyber risk. Q81 b) the Board should be regularly apprised of the insurer's cyber risk profile to ensure that it remains consistent with the insurer's risk tolerance as well as the insurer's overall business objectives. (add `Senior management, in consultation with the Board as appropriate',remove `As part of this responsibility, the Board') should consider whether the changes to the insurer's products, services, policies or practices, and the threat landscape materially affect its cyber risk profile. GA comment: Sections 81 a) and b) both overweight's the role of, and assigns too much responsibility to, the Board. In both instances, Senior Management will necessarily be involved in decisions around setting the firm's tolerance for cyber risk as well as considerations around changes to products, services, policies or practices in light of the company's cyber risk profile.	Paragraph 81(a) has been revised accordingly. Please see response to Comment 43.
41. General Insurance Association of Japan	Japan	No	Comment on 81.a. and b. See our comment on 48.d. Comment on 81.d. See our comment on 48.d. Considering that it could be difficult in some countries to secure members with appropriate skills, this paragraph should be revised as follows; d. An insurer's Board and senior management should cultivate awareness of and commitment to cybersecurity. The Board and senior management should make the effort to include members with skills appropriate to their oversight and management roles with respect to the risks posed by cyber threats. In addition, the Board and senior management should promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity and lead by	Please see responses to Comments 37 and 38. No change made. Other revisions reflect that the recommendations are not prescriptive.

			example. Comment on 81.f. Although this paragraph alludes to the independence of the roles of senior executives, we understand that various forms of governance are allowed depending on the insurers' scale of business, complexity, and the characteristics of its business in accordance with the principle of proportionality stipulated in section 1.3.	Please see response to Comment 37.
43. ACLI	United States	No	Governance is key when establishing cybersecurity within an insurer. However, ACLI believes that the IAIS inappropriately tasks a company's Board of Directors in setting cyber strategy at an insurer. In paragraph 81(a), the IAIS states that the Board is "ultimately responsible" for strategy. ACLI believes that the ultimate responsibility of cyber strategy and implementation of the strategy should be on senior management, which can oversee the day-to-day functions of a company. Senior management would also have additional flexibility to adjust to emerging cyber threats. We would similarly request that paragraph 81(b) be changed to read; "the Board should be regularly apprised of the insurer's cyber risk profile to ensure that it remains consistent with the insurer's risk tolerance as well as the insurer's overall business objectives. Senior management, in consultation with the Board as appropriate, should consider whether the changes to the insurer's products, services, policies or practices, and the threat landscape materially affect its cyber risk profile."	Please see response to Comment 40. Paragraph 81(b) has been revised accordingly.
44. American Insurance Association	United States of America	No	It is essential to accurately reflect the role of the Board in the Applications Paper. Unfortunately, there are elements of Paragraph 81 that expand the role of the Board beyond oversight and awareness to one of implementation. Additionally, particularly in the global context, we believe it is important to recognize the role of the Board in a group structure. We respectfully urge the following amendments: (a) The insurer's Board should be ultimately responsible for setting strategy and ensuring that cyber risk is effectively managed. The Board, IN CONJUNCTION WITH SENIOR MANAGEMENT, should OVERSEE the insurer's cybersecurity framework and set the insurer's tolerance for cyber risk. In a group setting, the insurer's parent Board or senior management may be responsible for setting the	Please see response to Comments 17, and 40 through 43.

			risk tolerance. IN A GROUP SETTING, THE INSURER'S PARENT BOARD OR SENIOR MANAGEMENT MAY BE RESPONSIBLE FOR SETTING THE RISK TOLERANCE. (b) Further, the Board should be regularly apprised of the insurer's cyber risk profile to ensure that it remains consistent with the insurer's risk tolerance as well as the insurer's overall business objectives. SENIOR MANAGEMENT, IN CONSULTATION WITH the Board AS APPROPRIATE, should consider whether changes to the insurer's products, services, policies or practices, and the threat landscape materially affect its cyber risk profile. Further, consistent with the principles of proportionality and risk, we recommend striking the reference to a Chief Information Security Officer (CISO). We agree that identifying an individual(s) with overall accountability for the cybersecurity framework is important, but for some mid- and small-size companies it may not be feasible to place this person at the C-Suite level as is suggested by the reference to "Chief Information Security Officer." Our proposed language is highlighted in caps above and we deleted the reference to "endorse" and "as part of this responsibility."	
45. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest changing the introductory paragraph sentence as follows: "With regard to cybersecurity governance, supervisory practices may encourage or reflect the following, where appropriate".	Please see response to Comment 10.
Q86 Comment on Paragraph 82				
Q87 Comment on Paragraph 83				
Q88 Comment on Paragraph 84				
Q89 Comment on Paragraph 85				
Q90 Comment on Paragraph 86				
Q91 Comment on Paragraph 87				

Q92 Comment on Paragraph 88				
Q93 Comment on Paragraph 89				
Q94 Comment on Paragraph 90				
Q95 Comment on Paragraph 91				
Q96 Comment on Paragraph 92				
Q97 Comment on Paragraph 93				
Q98 Comment on Paragraph 94				
Q99 Comment on Paragraph 95				
Q100 Comment on Paragraph 96				
Q101 Comment on Paragraph 97				
Q102 Comment on Paragraph 98				
46. AIA Group	Hong Kong	No	We agree that the focus of a risk assessment should take into account all reasonably foreseeable and relevant material risks. The paper should also recognise that these risks may vary from jurisdiction to jurisdiction and may depend on the nature, scale and complexity of the insurer. For example, there may be different risks associated with the sale of certain products i.e. through a digital website, than through licensed intermediaries.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
Q103 Comment on Paragraph 99				
47. Institute of International Finance	Global	No	[No comments submitted.]	No resolution required.
Q104 Comment on Paragraph 100				

Q105 Comment on Paragraph 101				
Q106 Comment on Paragraph 102				
Q107 Comment on Paragraph 103				
48. Association of Bermuda Insurers and Reinsurers	Bermuda	No	Included in the recommendations for supervisors regarding risk and control assessment is guidance regarding insurers responsibility to manage its exposure to cyber risk via third party service providers. The guidance suggests that the management of these risk should include the verification that third- party service providers "have implemented appropriate administrative, technical and physical measures to protect and secure the data…". ABIR considers this language may prove to be onerous and not reasonable depending on the extent and nature of the service being provided. We recommend the IAIS consider using language that allows for an insurer or group to conduct a level of due diligence proportionate to the nature of the service provided.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
49. Global Federation of Insurance Associations	Global	No	GFIA encourages the IAIS to consider qualifying language in subparagraphs m, n, and o regarding requirements to verify the security measures implemented by third-party vendors. Given the size and/or nature of the service a third-party vendor may provide, it may not be necessary or possible for an insurer to verify the cybersecurity protocols of every third-party service provider. While the security procedures of some vendors may be very important, for example a data storage vendor, not all third-party vendors provide services of a critical or sensitive nature with regard to cybersecurity.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
50. Institute of International Finance	Global	No	a) We would urge that a risk-based approach be introduced into this guidance. c) We would urge that a risk-based approach be incorporated into this guidance. d) Depending upon the size of the insurer, the interdependencies associated with third party service providers are potentially vast and do not all pose the same level of risk. We would therefore urge that a risk-based approach be incorporated into this guidance. e) We would urge that a risk-based approach be introduced into this guidance. g) We would urge that a risk-based approached be integrated into this requirement.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.

			We also would suggest a slight change to the language in the first sentence, replacing the word "integrate" with "coordinate".	Concur and revised accordingly.
51. AIA Group	Hong Kong	No	While we agree with the objectives of the risk and control assessment, we recommend that for large global enterprises it is not practical for all assets and that the classification and inventory related controls be focused primarily on critical assets for sub-paragraphs c, d, e. These requirements under paragraph 103 are extensive and prescriptive. There also does not appear to a materiality element. We suggest that it be clarified in this paragraph that what is appropriate for a particular insurer be applied to such an insurer and that a concept of materiality be incorporated. It would also be helpful to expand in paragraph 103c. on what the term "criticality" could mean as this is not clear. Would this be equivalent to whether the risk is considered "material"?	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
52. The Geneva Association	International	No	Para 103a: (add `To the extent practicable and based on risk', insurers should identify and classify functions including information assets and data sensitivity, as well as their interconnectedness; proactive technology and processes; external dependency management; and situational awareness. Explanation GA to above suggested change: We would urge that a risk-based approach be introduced into this guidance. 103 c) To the extent practicable (add `and based on risk'), the insurer should identify and maintain a current inventory or mapping of its information assets and system configurations, including interconnections with other internal and external systems, in order to know at all times the assets that support its business functions and processes. The insurer should carry out a risk assessment of those assets and classify them in terms of their criticality. Explanation to above suggested edit: We would urge that a risk-based approach be incorporated into this guidance. 103 d) As part this mapping exercise, (add `based on risk'), the insurer should also identify interdependencies in its information assets and system configurations, for example, from third party service providers. Comment to above change: depending upon the size of the insurer, the	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.

			interdependencies associated with third party service providers are potentially vast and do not all pose the same level of risk. We would therefore urge that a risk-based approach be incorporated into this guidance. 103 e) (add `Based on risk'), the inventory should encompass hardware, software platforms and applications, devices, systems, data, personnel, external information systems, critical processes, and documentation on expected data flows. Comment: We would urge that a risk-based approach be introduced into this guidance. 103 g) (add `Following a risk-based approach'), insurers should coordinate (remove: `integrate') identification efforts (i.e., identifying and maintaining an up-to-date record of both individual and system access rights) with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its list of critical business processes, functions, individual and system credentials, as well as its inventory of information assets to ensure that they remain current, accurate and complete. Comment: We would urge that a risk-based approached be integrated into this requirement. We also would suggest a slight change to the language in the first sentence, replacing the word "integrate" with "coordinate, as indicated above. Implementation of Proactive Technology and Processes 103 l. (add: `Taking a risk-based approach', insurers should protect data both when at-rest, in-transit and in-storage commensurate with the criticality of the information held and associated classification, extending to backup systems and offline data stores as well. Management of External Dependencies 103 m. Insurers should actively manage cyber risks presented by third parties (add: `based on risk'). For example, many insurers' systems and processes are directly or indirectly interconnected with numerous third parties, including cloud service providers and providers of outsourced functions. The cybersecurity of those entities	Please see response to Comment 50.

			may significantly affect the cyber risk that an insurer faces. Comment: Depending upon the size of its ecosystem, an insurer may have hundreds of third party service providers which do not all pose the same level of risk. A risk-based approach will necessarily be adopted to manage all the interconnections.	
53. General Insurance Association of Japan	Japan	No	Comment on 103.e. As for managing elements and forms of the inventory, management techniques that insurers judge appropriate should be allowed rather than uniformly requiring all insurers to encompass all the information into a single inventory. Therefore, this paragraph should be revised as follows; The inventory may encompass hardware, software platforms and applications, devices, systems, data, personnel, external information systems, critical processes, and documentation on expected data flows, based on the management method deemed appropriate by the insurer. Comment on 103.g. We assume it is immensely difficult to literally "integrate" identification efforts with other relevant processes in a narrow sense. Therefore, insurers should be allowed to interpret this paragraph as "insurers should manage identification efforts in association with other relevant processes", such as acquisition and change management, in order to facilitate a regular review of its list of critical business processes, functions, individual and system credentials, as well as its inventory of information assets to ensure that they remain current, accurate and complete. Comment on 103.q. As each insurer may have a different perception of "cyber events considered unlikely to occur or have never occurred in the past", we would like to make sure that the judgment of cyber threats to be considered is left to the discretion of each insurer.	Please see response to Comment 7 and 10. Please see response Comment 50. Noted.

55. ACLI	United States	No	ACLI would again encourage the IAIS to align its guidance with its intent to have risk-based and non-prescriptive requirements. Paragraph 103(a) should begin with the phrase: "To the extent practicable and based on risk..." Paragraph 103(c), paragraph 103(d), and paragraph 103(e) should similarly include the term "To the extent practicable and based on risk" Paragraph 103 (l), the IAIS determines that insurers should protect data that is at-rest, in-transit, and in-storage commensurate with the criticality of the information…" ACLI certainly believes that it is essential to protect critical consumer data. However, the scope of the IAIS guidance is immense, with many insurers having legacy technology systems that would be nearly impossible to implement the guidance the IAIS envisions Paragraph 103(m) should include a qualifier to read: "Insurers may actively management cyber risks presented by third parties, based on risk..." The first sentence of Paragraph 103(g) should read: "Following a risk-based approach, insurers may coordinate..." The IAIS also states in paragraph 103(n) that insurers verify that third-party service providers have implemented safeguards to secure data to the same degree expected of the insurer. Often, insurers are in no reasonable position to negotiate with service providers that are much larger (e.g. cloud service providers like Amazon) to audit whether their safeguards are adequate. ACLI recommends deletion of the subsection (n) from paragraph 103.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10. No change made.
56. American Insurance Association	United States of America	No	Wherever the Application Paper addresses measures or controls that a licensee should consider, the importance of the principles of flexibility, proportionality, and risk cannot be overstated. That is the foundation for the following recommendations for Paragraph 103. These would be in addition to, and not in lieu of, our suggestion in the general observations section to amend every introductory paragraph. Specifically, as it relates to subparagraph (n) we believe it is important to make sure	The word 'both' has been deleted from paragraph 103(l). Otherwise, please see response to Comment 55.

			that verification of a third-party's protective measures are consistent with risk since the requirements and assessment will vary based on the type and amount of sensitive data and system access the third party has. a. TO THE EXTENT PRACTICABLE AND BASED ON RISK, insurers should . . . . c. To the extent practicable AND BASED ON RISK, ... d. As part of this mapping process, TO THE EXTENT PRACTICABLE AND BASED ON RISK, the insurer should e. TO THE EXTENT PRACTICABLE AND BASED ON RISK, the inventory should. . . f. Insurers should identify and maintain, TO THE EXTENT PRACTICABLE, a current record of both individual and system access rights. . .and to use this information, TO THE EXTENT PRACTICABLE, both to ensure that access rights are no broader than necessary, and to facilitate identification . . . g. FOLLOWING A RISK-BASED APPROACH, insurers should COORDINATE . . . l. TO THE EXTENT PRACTICABLE AND BASED ON RISK, insurers should protect data when at-rest, in transit and in-storage commensurate with the criticality of the information held and associated classification, extending to back up systems and offline data stores as well. m. Insurers should manage cyber risks presented by third parties based on risk BASED ON RISK. n. TO THE EXTENT PRACTICABLE, Insurers should verify that third-party service providers have implemented appropriate administrative, technical, and physical measures to protect and secure the data of an insurer and its customers	

			CONSISTENT WITH THE INSURER'S RISK ASSESSMENT. . . . Our proposed language is highlighted in caps above and we deleted "integrate" in subparagraph g.; "both" in subparagraph l.; "actively" in subparagraph m.; and "to the same degree expected of the insurer" in subparagraph n.	
57. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest changing the introductory paragraph sentence as follows: "With regard to insurers' cybersecurity risk and control assessment, supervisory practices may encourage or reflect the following, where appropriate". Suggest removing 103(a) as 103(b) sufficiently captures the thought. Suggest changing 103(l) as follows: "Insurers should protect data both when at-rest, in transit and in storage throughout the data life cycle commensurate with the criticality of the information held and associated classification."	Please see response to Comment 10. Concur and revised accordingly. Please see revision to paragraph 103(l) in response to this and similar Comments.
Q108 Comment on Paragraph 104				
Q109 Comment on Paragraph 105				
Q110 Comment on Paragraph 106				
Q111 Comment on Paragraph 107				
Q112 Comment on Paragraph 108				
58. National Association of Insurance	USA, NAIC	No	There should just be one bold heading for each jurisdiction.	No revision necessary.

Commissioners (NAIC)				
Q113 Comment on Paragraph 109				
Q114 Comment on Paragraph 110				
Q115 Comment on Paragraph 111				
Q116 Comment on Paragraph 112				
59. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	There should just be one bold heading for each jurisdiction.	Please see response to 58.
Q117 Comment on Paragraph 113				
Q118 Comment on Paragraph 114				
Q119 Comment on Paragraph 115				
Q120 Comment on Paragraph 116				
Q121 Comment on Paragraph 117				
Q122 Comment on Paragraph 118				
Q123 Comment on Paragraph 119				
60. American Insurance Association	United States of America	No	Section 4D of the NAIC Insurance Data Security Model Law is categorized as listing requirements for managing risk, based on the insurer's ongoing risk assessment. We believe this should be amended to state that the Model Law lists recommendations rather than requirements. Each of the measures identified and the process for implementation shall be based on the insurer's risk assessment. We recommend this change to avoid any confusion as to the role of the risk assessment and the measures that an insurer implements. We have a similar observation for the categorization of the NYDFS Cybersecurity Regulation. If the	No change necessary. The IAIS notes the NAIC description of its model.

			change from requirements to recommendations is not acceptable to the drafters, we would recommend language that suggests broad categories of measures are required to be considered and how the specific measures for implementing each category are the decision of the insurer based on its risk assessment. Recommended language: Section 4C of the NAIC Insurance Data Security Model Law requires the insurer to perform an ongoing risk assessment and Section 4D lists RECOMMENDED MEASURES for managing risk, based on the insurer's ongoing risk assessment. Alternatively, we would suggest: Section 4C of the NAIC Insurance Data Security Model Law requires the insurer to perform an ongoing risk assessment and Section 4D lists BROAD CATEGORIES OF MEASURES REQUIRED TO BE CONSIDERED for managing risk, based on the insurer's ongoing risk assessment. Our proposed language is highlighted in caps above and we deleted the references to "requirements" twice.	
Q124 Comment on Paragraph 120				
Q125 Comment on Paragraph 121				
Q126 Comment on Paragraph 122				
Q127 Comment on Paragraph 123				
Q128 Comment on Paragraph 124				
Q129 Comment on Paragraph 125				
Q130 Comment on Paragraph 126				
Q131 Comment on Paragraph 127				
Q132 Comment on Paragraph 128				
Q133 Comment on Paragraph 129				

61. Institute of International Finance	Global	No	While we support the language in para.129, we would like to provide the following example to illustrate how "appropriately independent' can be done in practice: "As an example, it is a common practice for security organizations to perform "red team" exercises - wherein the red team (normally a third party) performs highly sophisticated attacks, acting as an attacker, of the environment. If the CISO isn't aware of and overseeing these activities, the organization may take steps which impact the business (e.g., turning off business systems which have been compromised by the tester). These steps are appropriate in a real attack, but with a test the general practice is to halt the testing before taking such steps. General practices are to make sure the test has appropriate independence to meet the objective, but for them to still run under the auspices of the CISO. Reports from such exercises are often shared with 2nd and 3rd line functions."	Noted.
Q134 Comment on Paragraph 130				
Q135 Comment on Paragraph 131				
Q136 Comment on Paragraph 132				
Q137 Comment on Paragraph 133				
62. Institute of International Finance	Global	No	j) An effective intrusion detection capability could assist insurers in identifying deficiencies in their protective measures for early remediation. These capabilities could include, for example, data loss/leaks prevention and detection, the recording and documentation of audit logs, event data aggregation, correlation, analysis and communication, as well as network, personnel and external dependency activity monitoring.	Concur and revised based on this and similar Comments.
63. AIA Group	Hong Kong	No	Similar to our comment on paragraph 103, the requirements under this paragraph 133 are extensive and prescriptive. Again there does not appear to be a materiality element. We similarly suggest clarification for this paragraph that only what is appropriate for a particular insurer be applied to such an insurer and that a concept of materiality be incorporated. It would not make sense if extensive testing was required if there was minimal risk.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.

64. The Geneva Association	International	No	would suggest a minor change in wording as indicated below : Para 133 j) An effective intrusion detection capability could assist insurers in identifying deficiencies in their protective measures for early remediation. These capabilities (add`could' remove `would ') include, (add: `for example', data loss/leaks prevention and detection, the recording and documentation of audit logs, event data aggregation, correlation, analysis and communication, as well as network, personnel and external dependency activity monitoring.	Please see response to Comment 62.
65. General Insurance Association of Japan	Japan	No	Comment on 133.f. The definition of the "cyber threat intelligence programme" should be clarified. Comment on 133.n. We would like to have a detailed definition of "advanced threat agent capabilities". Comment on 133.o. See our comment on 48.d. Comment on 133.s. Penetration tests are usually carried out by a limited number of (mainly IT) departments. We would like to have a clearer view of how "the tests which could include wider business stakeholders" will be carried out.	Please refer to the relevant section of CPMI/IOSCO Guidance. Please see response to comment on 48(d). The manner of conducting penetration testing is beyond the scope of the Application Paper.
66. ACLI	United States	No	ACLI again understands much of the rationale for the IAIS, but much of its guidance is onerous. Under paragraph 133(b), the IAIS provides for real-time or near-real time continuous monitoring of threats by insurers. ACLI has significant concerns about the resources necessary for this capability, especially at smaller insurance companies. The IAIS must ensure that its guidance can be tailored to insurers of all sizes and in relation to the threats they face. ACLI recommends the deletion of paragraph 133(b).	Paragraph 133(b) has been revised to state that an “insurer should consider establishing…” rather than “should establish.”

			Much of the guidance put forward in this section is simply not scalable. Specifically, ACLI has significant concerns with paragraph 133(i), 133 (j) and paragraph 133(p). The use of terminology of "state-of-the-art" is not defined and can mean a host of different things. Therefore, ACLI again recommends that the IAIS revisit these sections and consider making them more risk-based. If that is not possible, we recommend deletion of these sections.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
67. American Insurance Association	United States of America	No	Continuing with our risk-based amendments we offer the following edits to paragraph 133. . . . . g. As part of the monitoring process, insurers should manage the identities and credentials for physical, logical, and remote access to information assets, based on principles SUCH AS least privilege and separation of duties. i. The insurers should have the ability to detect an intrusion early, as this capability is critical for swift containment and recovery. Insurers should CONSIDER a defence-in-depth approach by instituting multi-layered detection controls covering people, processes, and technology, with each layer serving as a safety net for preceding layers. j. . . .These capabilities WOULD include, FOR EXAMPLE, data loss/leaks prevention and detection, ... s. Insurers should CONSIDER carryING out penetration tests to identify vulnerabilities that may affect. . . Our proposed language is highlighted in caps above and we deleted "take" and "would."	Concur and Paragraph 133 (g) has been revised accordingly. The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10. Please see response to Comments 61 - 66.

68. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest changing the introductory paragraph sentence as follows: "With regard to insurers' cybersecurity monitoring, supervisory practices may encourage or reflect the following, where appropriate".	Please see response to Comment 10.
			Suggest changing the third sentence of 133(b) to: "Insurers may consider establishing a SOC or developing similar capability to provide round the clock monitoring, adaptively maintaining and testing SOC capabilities."	Concur and revised.
			Suggest changing the second sentence of 133(n) to: "For example, insurers may consider establishing an appropriately comprehensive testing programme…"	Concur and revised.
			133(q-t) should be included as sub bullets underneath 133(p) and not as separate sections.	Concur and revised.
Q138 Comment on Paragraph 134				
Q139 Comment on Paragraph 135				
Q140 Comment on Paragraph 136				
Q141 Comment on Paragraph 137				
Q142 Comment on Paragraph 138				
Q143 Comment on Paragraph 139				
Q144 Comment on Paragraph 140				
Q145 Comment on Paragraph 141				
Q146 Comment on Paragraph 142				
Q147 Comment on Paragraph 143				

Q148 Comment on Paragraph 144				
Q149 Comment on Paragraph 145				
Q150 Comment on Paragraph 146				
Q151 Comment on Paragraph 147				
Q152 Comment on Paragraph 148				
69. American Insurance Association	United States of America	No	We recommend the following amendment to this paragraph: "Section 4D of the NAIC Insurance Data Security Model Law directs the insurer to CONSIDER network monitoring among its potential security measures. . ." Our proposed language is in caps above and we deleted "include."	No change necessary. The IAIS notes the NAIC description of its model.
Q153 Comment on Paragraph 149				
Q154 Comment on Paragraph 150				
Q155 Comment on Paragraph 151				
Q156 Comment on Paragraph 152				
Q157 Comment on Paragraph 153				
Q158 Comment on Paragraph 154				
Q159 Comment on Paragraph 155				
Q160 Comment on Paragraph 156				
Q161 Comment on Paragraph 157				
Q162 Comment on Paragraph 158				
Q163 Comment on Paragraph 159				
Q164 Comment on Paragraph 160				

70. AIA Group	Hong Kong	No	As above, our comment on paragraph 160 is similar to our comments on paragraph 103 and 133 in respect of prescriptiveness and materiality. All these requirements should take into consideration the nature, scale and complexity of the insurer. For example, if there is a non-material incident (such as the loss of a password protected phone with embedded and appropriate security measures to remotely wipe any personal data on the phone), it would not necessarily warrant a full blown stakeholder communication.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
71. The Geneva Association	International	No	We suggest to add the following additional language: Para 160 k) Insurers should have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative process, (add: `as appropriate depending on the risk posed by the incident'). In this regard, insurers should establish relevant system logging policies that include the types of logs to be maintained and their retention periods. While forensic analysis may need to be postponed and ICT resources may be focused on recovering critical systems, insurers should ensure that investigations can still be performed post-event to the extent possible, e.g., through preservation of necessary system logs and evidence.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10. No change made.
72. General Insurance Association of Japan	Japan	No	Comment on 160.e. We would like to more clearly understand the objective of the rule "insurers should plan to have access to external experts". Does it require insurers to conclude some kind of contract with third-parties in advance of a large-scale or industry-wide event to avoid the risk of losing access to external resources? Comment on 160.f. We would like to know the intention behind the IAIS requiring insurers to consult and coordinate with relevant authorities regarding their response plan. This requirement seems too prescriptive. Comment on 160.h.	Local supervisors and firms are better positioned to address whether and how this recommendation 160(e) may be implemented. This application paper does not state any requirements. The IAIS suggests it is good practice for supervisors to consider verifying that insurers have in place appropriate response plans.

			As long as the necessary responsibilities with regard to stakeholder communications are clarified, we do not think insurers need to have "a specific team" in place for all stakeholder communications.	Noted.
74. ACLI	United States	No	ACLI agrees with the IAIS about the importance of a response following a successful cybersecurity incident. ACLI again stresses that the IAIS should enable insurers to tailor their cyber protections to best meet their risks. ACLI has significant concerns with Paragraph 160(h), which discusses the team an insurer must have in place to respond to a breach. ACLI stresses to the IAIS that any response to a cybersecurity incident is greatly dependent on individual facts. Allowing insurers, the greatest amount of flexibility in this space would be the most prudent. As a first step, ACLI requests that the IAIS remove the term "should" and instead consider using the term "may." ACLI would also encourage the IAIS to include language that states that any notification to a cybersecurity event should apply only to events reasonably likely to cause material harm to a company or other insurance licensee or to consumers whose sensitive personal information is reasonably believed to have been involved in the event. This would reduce the occurrences in which insurers are notifying consumers over incidents that cause no real harm. ACLI also recommends amending paragraph 106(k) to read "Insurers should have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigation process, as appropriate depending on the risk posed by the incident." The inclusion of the latter language again ensures that companies can react to threats in a risk-based and flexible manner.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10. Recommendation 160(h) modified to indicate that insurers “should consider having in place” a specific communication team. Reporting per local law is addressed in Recommendation 160(j). Please see response to Comment 71.
75. American Insurance Association	United States of America	No	A risk-based approach necessitates the amendments identified below. For instance, while it makes sense for all employees to have an awareness of the risk, the level of training will differ based on their respective roles in the company and access to information and information systems. Similarly, investigation, analysis and logging are important practices but the extent to which these activities are executed should depend on the insurer's risk analysis. Recommendations: a. In advance of a cybersecurity incident, insurers should raise awareness among	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.

			all its stakeholders by providing training for employees and others with access to its systems BASED ON RISK. . . . k. Insurers should have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative process, AS APPROPRIATE DEPENDING ON THE RISK POSED BY THE INCIDENT. Our proposed language is highlighted in caps above.	Also please see an additional sentence in Paragraph 160 (a).
76. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest changing the introductory paragraph sentence as follows: "With regard to insurers' cybersecurity response, supervisory practices may encourage or reflect the following, where appropriate".	Please see response to Comment 10.
Q165 Comment on Paragraph 161				
Q166 Comment on Paragraph 162				
Q167 Comment on Paragraph 163				
Q168 Comment on Paragraph 164				
Q169 Comment on Paragraph 165				
Q170 Comment on Paragraph 166				
Q171 Comment on Paragraph 167				
Q172 Comment on Paragraph 168				
Q173 Comment on Paragraph 169				
Q174 Comment on Paragraph 170				
77. American Insurance Association	United States of America	No	Consistent with the approach to proportionality and risk-based approaches to cybersecurity, we recommend that "any identified incidents" in the first paragraph be amended to state instead "defined cybersecurity events." We also would	In first sentence, NAIC has replaced “any identified incidents” with “defined cybersecurity events.” In

			recommend clarifying that the notification obligations in Section 6 are based on specific triggers and not every potential identified incident is required to be reported.	second sentence, replaced “incident” with “defined cybersecurity event.”
Q175 Comment on Paragraph 171				
Q176 Comment on Paragraph 172				
Q177 Comment on Paragraph 173				
Q178 Comment on Paragraph 174				
Q179 Comment on Paragraph 175				
Q180 Comment on Paragraph 176				
Q181 Comment on Paragraph 177				
Q182 Comment on Paragraph 178				
Q183 Comment on Paragraph 179				
Q184 Comment on Paragraph 180				
78. Institute of International Finance	Global	No	We would suggest that preconceived plans or procedures for recovery from a cybersecurity incident will take a risk-based approach. For example, high-risk systems and processes, as opposed to all systems and processes, could be designed to maintain an uncorrupted "golden copy". Similarly, a risk-based approach will be used to safeguard, protect, etc., data. Finally, the insurers' cybersecurity framework will take a risk-based approach in terms of its data recovery measures. Suggested change: 180 a) Insurers should have in place (add "risk-based" strike "validate") plans and procedures to recover from a cybersecurity incident. c) Insurers should design and test their systems and processes to enable timely recovery of accurate data following a breach. As an example, (add "high-risk")	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10. The word “validated” has been deleted from Paragraph 180(a). Recommendation 160(c) has been amended for consistency.

			insurers' systems and processes could be designed to maintain an uncorrupted "golden copy" of critical data (including, to the extent possible, application source code) to be used in the restoration of impacted systems and data. Data instances should be safeguarded by stringent protective and detective controls, (add "based on risk"). In addition, the insurers' cybersecurity framework should include data recovery measures, such as keeping a backup copy of all policyholder data in the event such data is corrupted, (add "based on risk").	
79. The Geneva Association	International	No	We would suggest that preconceived plans or procedures to recovery from a cybersecurity incident will take a risk-based approach. For example, high-risk systems and processes, as opposed to all systems and processes, could be designed to maintain an uncorrupted "golden copy". Similarly, a risk-based approach will be used to safeguard, protect, etc., data. Finally, the insurers' cybersecurity framework will take a risk-based approach in terms of its data recovery measures. 180 a) Insurers should have in place (add: `risk-based' remove `validated') plans and procedures to recover from a cybersecurity incident. 180 c) Insurers should design and test their systems and processes to enable timely recovery of accurate data following a breach. As an example, (add: `high-risk' insurers' systems and processes could be designed to maintain an uncorrupted "golden copy" of critical data (including, to the extent possible, application source code). To be used in the restoration of impacted systems and data. Data instances should be safeguarded by stringent protective and detective controls, (add: `based on risk'). In addition, the insurers' cybersecurity framework should include data recovery measures, such as keeping a backup copy of all policyholder data in the event such data is corrupted, (add: `based on risk').	Please see response to Comment 78.
80. ACLI	United States	No	ACLI recommends that paragraph 180(a) be amended to read: " Insurers may have in place risk-based plans and procedures to recover from a cybersecurity incident." We further request the changes to 180(c) so it may be more risk-based and read "Insurers may design and test their systems and processes to enable timely recovery of accurate data following a breach. As an example, high-risk insurers' systems and processes could be designed to maintain an uncorrupted "golden	Please see response to Comment 78.

			copy" of critical data (including, to the extent possible, application source code). To be used in the restoration of impacted systems and data. Data instances should be safeguarded by stringent protective and detective controls, based on risk. In addition, the insurers' cybersecurity framework should include data recovery measures, such as keeping a backup copy of all policyholder data in the event such data is corrupted, to the extent practicable based on risk."	
81. American Insurance Association	United States of America	No	We question the use of the term "validated" in subparagraph a. Insurers can prepare plans and procedures to recover from a cybersecurity incident and conduct tests as is referenced earlier in the Applications Paper, but no two cyber incidents may be the same. It seems overly burdensome to require that plans and procedures be "validated." Instead we recommend replacing "validated" with "risk-based." Subparagraph (a) would read: Insurers should have in place RISK-BASED plans and procedures to recover from a cybersecurity incident. We also believe important risk qualifications are missing from subparagraph c and recommend the following: c. Insurers should design and test their systems and processes to enable timely recovery of accurate data following a breach. As an example, HIGH-RISK insures' systems and processes could be designed to maintain an uncorrupted "golden copy" of critical data (including, to the extent possible, application source code), to be sued in the restoration of impacted systems and data. Data instances should be safeguarded by stringent protective and detective controls, BASED ON RISK. In addition, the insurer's cybersecurity framework should include data recovery measures, such as keeping a backup copy of all policyholder data in the event such data is corrupted, TO THE EXTENT PRACTICABLE BASED ON RISK. Our proposed language is highlighted in caps above.	Please see response to Comment 78.
82. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest changing the introductory paragraph sentence as follows: "With regard to insurers' cybersecurity recovery, supervisory practices may encourage or reflect the following, where appropriate".	Please see response to Comment 10.
Q185 Comment on Paragraph 181				
Q186 Comment on Paragraph 182				

Q187 Comment on Paragraph 183				
Q188 Comment on Paragraph 184				
Q189 Comment on Paragraph 185				
Q190 Comment on Paragraph 186				
83. American Insurance Association	United States of America	No	Consistent with the approach to proportionality and risk-based approaches to cybersecurity, we recommend that "any identified incidents" in the first paragraph be amended to state "defined cybersecurity events." We also would recommend clarifying that the notification obligations in Section 6 are based on specific triggers and not every potential identified incident is required to be reported. Recommended language: As described above under the "response" element, Sections 4H of the NAIC Insurance Data Security Model Law requires the insurer to establish a written incident response plan that indicates how the insurer will respond to and recover from DEFINED CYBERSECURITTY EVENTS. The plan must include information on communications that need to take place in the event of an incident, how weaknesses will be remediated, the definition of clear roles, responsibilities, and levels of decision-making authority. Under Section 6, the insurer is required to notify, BASED ON SPECIFICALLY DEFINED TRIGGERS, the Commissioner (i.e., the State insurance supervisor), the affected consumers, and certain other stakeholders. Our proposed language is highlighted in caps above and we delete "any identified incidents."	In first sentence, NAIC has replaced “any identified incidents” with “defined cybersecurity events.” In second sentence, replaced “incident” with “defined cybersecurity event.”
Q191 Comment on Paragraph 187				
Q192 Comment on Paragraph 188				
Q193 Comment on Paragraph 189				
Q194 Comment on Paragraph 190				
Q195 Comment on Paragraph 191				

Q196 Comment on Paragraph 192				
84. Global Federation of Insurance Associations	Global	No	Information sharing of threat data is an important mitigation tool that GFIA supports. However, many insurance groups have legitimate concerns about data sharing around confidentiality issues and liability. The IAIS could expand this paper to discuss more fully the role that supervisors and non-supervisory governmental bodies can play in information sharing. Sharing information should not be limited to private entities, but should also involve reciprocal sharing from supervisory and other governmental bodies. GFIA understands that some governments are interested in collaborating with industry to provide a more comprehensive threat data sharing system between all relevant parties. The IAIS could have a positive role in supporting the development of such systems on both the national and international levels, and may want to encourage governments to consider involving non-supervisory governmental bodies in information sharing arrangements. A voluntary, public-private approach, with appropriate privacy and liability protections, to sharing collective threat information can be very beneficial.	Noted. This may be further taken into account in IAIS future work.
Q197 Comment on Paragraph 193				
Q198 Comment on Paragraph 194				
Q199 Comment on Paragraph 195				
Q200 Comment on Paragraph 196				
Q201 Comment on Paragraph 197				
Q202 Comment on Paragraph 198				
85. Institute of International Finance	Global	No	Depending upon the size of its third-party ecosystem, the insurer will necessarily take a risk-based approach in any decision to exchange information on its cybersecurity framework with relevant third-party service providers. Suggested change: 198 g) An insurer should consider exchanging information on its cybersecurity framework bilaterally with its third-party service providers to promote mutual understanding of each other's approach to security systems that are linked or	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.

			interfaced, (add "based on the risks related to the third party"). Such information exchange would facilitate an insurer's and its stakeholder's efforts at dovetailing their respective security measures to achieve greater cybersecurity.	
86. AIA Group	Hong Kong	No	We suggest clarifying that the recommendations under paragraph 198 are not mandatory as such information sharing networks are not well established in all locations. It should also be clear that all confidential information exchanged by supervisors or with other insurers should be bound by a strict confidentiality regime. A MoU on such confidentiality should be in place between supervisors before an exchange of confidential information is made. Also of note is that for listed companies there may be a prohibition on the disclosure of non-public company information unless the proposed recipient agrees to keep the information confidential and protect it from disclosure except where required by a court of competent jurisdiction or by law.	It is understood that in exchanging information supervisors and insurers are subject to relevant laws and regulations. Please refer to Paragraph 198(f), as well as the ICPs highlighted in Paragraph 197.
87. The Geneva Association	International	No	198 g) An insurer should consider exchanging information on its cybersecurity framework bilaterally with its third-party service providers to promote mutual understanding of each other's approach to security systems that are linked or interfaced, (add: `based on the risks related to the third party'). Such information exchange would facilitate an insurer's and its stakeholder's efforts at dovetailing their respective security measures to achieve greater cybersecurity. Comment: depending upon the size of its third party ecosystem, the insurer will necessarily take a risk-based approach in any decision to exchange information on its cybersecurity framework with relevant third-party service providers.	Please see response to Comment 85.
88. General Insurance Association of Japan	Japan	No	Comment on 198.a. We would like to make sure that insurers have the discretion as to whether to participate or not in FS-ISAC or Financials ISAC Japan, taking into account their judgment of the necessity to enhance the effectiveness of their cybersecurity. We also would like to make sure that the principle of proportionality is applied with regard to their decision on the necessity of such participation. Comment on 198.d., e., and f.	Please see response to Comment 85.

			This paragraph assumes that an insurer's cyber threat intelligence operations are a given. However, we would like to point out that in reality it is difficult to even have a department that deals with cyber threat intelligence operations. Comment on 198.g. We think that exchanging information "bilaterally" on their cybersecurity framework with third-party service providers is unrealistic. Such exchanges would be no different from exposing an insurer's security and governance risks, and would put insurers in greater danger with regard to their cybersecurity.	Paragraph 198, including 198(g), recommends that insurers "consider" participating in the described approaches to information sharing, which is consistent with current and emerging views on best practices.
89. ACLI	United States	No	We recommend that paragraph 198(g) be amended to read: "An insurer may consider exchanging information on its cybersecurity framework bilaterally with its third-party service providers to promote mutual understanding of each other's approach to security systems that are linked or interfaced, as appropriate based on the risks related to the third party. Such information exchange would facilitate an insurer's and its stakeholder's efforts at dovetailing their respective security measures to achieve greater cybersecurity."	Please see response to Comment 85.
90. American Insurance Association	United States of America	No	Information sharing is an important element of enhancing cyber resiliency; however, insures may not always be comfortable with the information sharing outlined in this paragraph. It should be up to the insurer to assess whether they want to share information with the industry and should not be encouraged or required to do so by the supervisor. To that end, our recommended edits to subparagraph 9 are intended to clarify the bi-lateral nature of the information exchange with third-parties and recognize that all information exchanges, including the material to be exchanged, should be risk-based given the potentially sensitive nature of the information. g. An insurer should consider BILATERAL INFORMATION EXCHANGES on its cybersecurity framework with its third-party service providers to promote mutual understanding of each other's approach to securing systems that are linked or interfaced, AS DETERMINED BY THE INSURER BASED ON THE RISKS RELATED TO THE THIRD PARTY. Such information exchange COULD facilitate	Please see response to Comment 85. The word "would" has been replaced with "could" in 198(g).

			an insurer's and its stakeholders' efforts at dovetailing their respective security measures to achieve greater cybersecurity. Our proposed language is in caps above and we delete: "exchanging information;" "bilaterally;" and "would."	
91. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest changing the introductory paragraph sentence as follows: "With regard to insurers' cybersecurity information sharing, supervisory practices may encourage or reflect the following, where appropriate".	Please see response to Comment 10.
Q203 Comment on Paragraph 199				
Q204 Comment on Paragraph 200				
Q205 Comment on Paragraph 201				
Q206 Comment on Paragraph 202				
Q207 Comment on Paragraph 203				
Q208 Comment on Paragraph 204				
Q209 Comment on Paragraph 205				
Q210 Comment on Paragraph 206				
Q211 Comment on Paragraph 207				
Q212 Comment on Paragraph 208				
Q213 Comment on Paragraph 209				
Q214 Comment on Paragraph 210				
Q215 Comment on Paragraph 211				
Q216 Comment on Paragraph 212				

Q217 Comment on Paragraph 213				
Q218 Comment on Paragraph 214				
Q219 Comment on Paragraph 215				
Q220 Comment on Paragraph 216				
Q221 Comment on Paragraph 217				
94. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Change reference to "FS-ISAC"	Typo corrected.
Q222 Comment on Paragraph 218				
Q223 Comment on Paragraph 219				
95. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	First sentence, this should be "Financial Services Sector Coordinating Council." Also, add the following: "Through the FBIIC, state insurance regulators and the NAIC collaborate with the U.S. Treasury and FSSCC to facilitate table top exercises to explore cybersecurity incident response and recovery across the insurance sector." In the current second sentence, change the reference to "Cybersecurity Forum for Independent and Executive Branch Regulators".	Paragraph 219 has been revised as the NAIC requested.
Q224 Comment on Paragraph 220				
Q225 Comment on Paragraph 221				
Q226 Comment on Paragraph 222				
Q227 Comment on Paragraph 223				
Q228 Comment on Paragraph 224				

Q229 Comment on Paragraph 225				
Q230 Comment on Paragraph 226				
Q231 Comment on Paragraph 227				
Q232 Comment on Paragraph 228				
Q233 Comment on Paragraph 229				
Q234 Comment on Paragraph 230				
96. AIA Group	Hong Kong	No	The requirements under paragraph 230 are extensive. It may not be practical or necessary for all insurers to comply with all these requirements. Our view is that it should be made clear that not all of these requirements are mandatory.	The Application Paper will reflect that as with all supervisory material, its guidance is offered against the backdrop principles of risk-based and proportionate application. Please see response to Comment 10.
97. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest changing the introductory paragraph sentence as follows: "With regard to insurers' cybersecurity continuous learning, supervisory practices may encourage or reflect the following, where appropriate".	Please see response to Comment 10.
Q235 Comment on Paragraph 231				
Q236 Comment on Paragraph 232				
Q237 Comment on Paragraph 233				
Q238 Comment on Paragraph 234				
Q239 Comment on Paragraph 235				
Q240 Comment on Paragraph 236				
Q241 Comment on Paragraph 237				

Q242 Comment on Paragraph 238
Q243 Comment on Paragraph 239
Q244 Comment on Paragraph 240
Q245 Comment on Paragraph 241
Q246 General comments on Section 4:
Q247 Comment on Paragraph 242
Q248 Comment on Paragraph 243
Q249 Comment on Paragraph 244
Q250 Comment on Paragraph 245
Q251 Comment on Paragraph 246
Q252 Comment on Paragraph 247
Q253 Comment on Paragraph 248
Q254 Comment on Paragraph 249
Q255 Comment on Paragraph 250
Q256 General comments on Section 5:
Q257 Comment on Paragraph 251
Q258 Comment on Paragraph 252
Q259 Comment on Paragraph 253
Q260 Comment on Paragraph 254
Q261 Comment on Paragraph 255

Q262 Comment on Paragraph 256				
Q263 Comment on Paragraph 257				
Q264 Comment on Paragraph 258				
Q265 Comment on Paragraph 259				
Q266 Comment on Paragraph 260				
Q267 Comment on Paragraph 261				
Q268 Comment on Paragraph 262				
Q269 Comment on Paragraph 263				
Q270 Comment on Paragraph 264				
Q271 Comment on Paragraph 265				
Q272 Comment on Paragraph 266				
Q273 Comment on Paragraph 267				
Q274 Comment on Paragraph 268				
Q275 General comments on Section 6:				
Q276 Comment on Paragraph 269				
Q277 Comment on Paragraph 270				
98. AIA Group	Hong Kong	No	We appreciate and agree the reiteration in this paragraph of the proportionality principle. Our hope is that this principle could be replicated more throughout the paper particularly where certain elements may be taken or misinterpreted as prescriptive requirements.	This is noted and has been taken into account in the revisions described in the responses to comments above. In addition Paragraph 270 has been revised to recognize the principle of risk-based application.

Q278 Comment on Paragraph 271
Q279 Comment on Paragraph 272
Q280 Comment on Paragraph 273