GIAJ comments on the IAIS consultation on "Draft Application Paper on Supervision of Insurer Cybersecurity"

Section/Paragraph	
General comments on the Application Paper	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. 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.
Comment on Paragraph 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.
Comment on Paragraph 81.a	See our comment on 48.d.
Comment on Paragraph 81.b	See our comment on 48.d.

Comment on Paragraph 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 example.
Comment on Paragraph 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.
Comment on Paragraph 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 Paragraph 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 Paragraph 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.
Comment on Paragraph 133.f	The definition of the “cyber threat intelligence programme” should be clarified.
Comment on Paragraph 133.n	We would like to have a detailed definition of “advanced threat agent capabilities”.
Comment on Paragraph 133.o	See our comment on 48.d.
Comment on Paragraph 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.
Comment on Paragraph 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 Paragraph 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 Paragraph 160.h	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.
Comment on Paragraph 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 Paragraph 198.d	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 Paragraph 198.e	See our comment on 198.d.
Comment on Paragraph 198.f	See our comment on 198.d.
Comment on Paragraph 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.