Questions	Comments
1	We understand that this application paper does not establish new supervisory objectives, but rather summarizes existing ICP provisions from an operational resilience perspective. As there is no definitive solution to the issue of operational resilience, we ask that the IAIS continue to share the status of its deliberations on this topic with insurers as appropriate. We ask for continued consistency in the development of the draft Toolkit and the drafting of the AP regarding supervisory practices in late 2024.
2	We are aware that the existing APs contain language such as "APs do not set new standards or expectations, but provide supporting material to assist in the implementation of existing standards". We request that it be clearly stated in this AP as well.
10	As the term "operational resilience" is used extensively in various parts, it should be redefined (or reposted) and clarified in this AP.
11	We expect that a proportional approach will be adopted in the development of supervisory practices in late 2024, taking into account regional and jurisdictional circumstances, rather than adding new requirements, etc.
31	Since operational disruption/impact is not always quantifiable, we suggest replacing "Quantifies" in the first bullet point with "Understands" or additionally describing that there are cases where it is impossible to quantify maximum disruption/impact. The second bullet point: Regarding "pre-defined", we would like to clarify this means that each entity defines its own "tolerances".
32	We agree on the importance of scenario testing with severe but plausible scenarios. On the other hand, it is not easy to prepare exhaustive scenarios because there are many possible factors that can affect operational resilience. Scenario testing is only one of various ways to improve operational resilience, and therefore, instead of preparing exhaustive scenarios, only those scenarios that are truly probable and important should be carefully selected for implementation.
36	In light of the NIST (National Institute of Standards and Technology) and other general frameworks, it is appropriate to have "identification" before "protection, detection, response, and recovery".
37	- Paragraph 23 in general is very detailed. In addition, various perspectives are described in parallel in bullet points, making it difficult to understand what kind of response will be required. For example, regarding the first bullet point, what is the intention of selecting these categories among many security measures? If internationally used standards are referred to, we suggest clarifying the source and adding a sentence such as "For example, the following approaches could be considered with reference to...". - Generally, measures by people/policies/technologies are considered to be effective. Based on the premise that this paragraph is intended to provide examples, we suggest adding a policy perspective.

41	- Regarding "clear recovery objectives", is it correct to understand that insurers are to set RPO(Recovery Point Objective), RTO(Recovery Time Objective), etc., which they consider appropriate? - Insurers are not supposed to validate testing of the BCPs of third parties. In this context, is "confirmation of test results" synonymous with "validation"?
42	We suggest replacing "manages" with "oversees". (The second bullet point also mentions "Supports effective management...".)
51	Paragraph 30 (first bullet point): It is important to enhance the resilience of the entire industry through information sharing. On the other hand, because matters related to operational resilience could also provide useful hints to cyber attackers, the scope of stakeholders should be carefully limited as necessary when collaborating and transparently communicating with them. Therefore, we suggest adding "taking into account confidentiality" at the end of the sentence.