European Union Aviation Safety Agency

FAQ n.139288

FAQs:

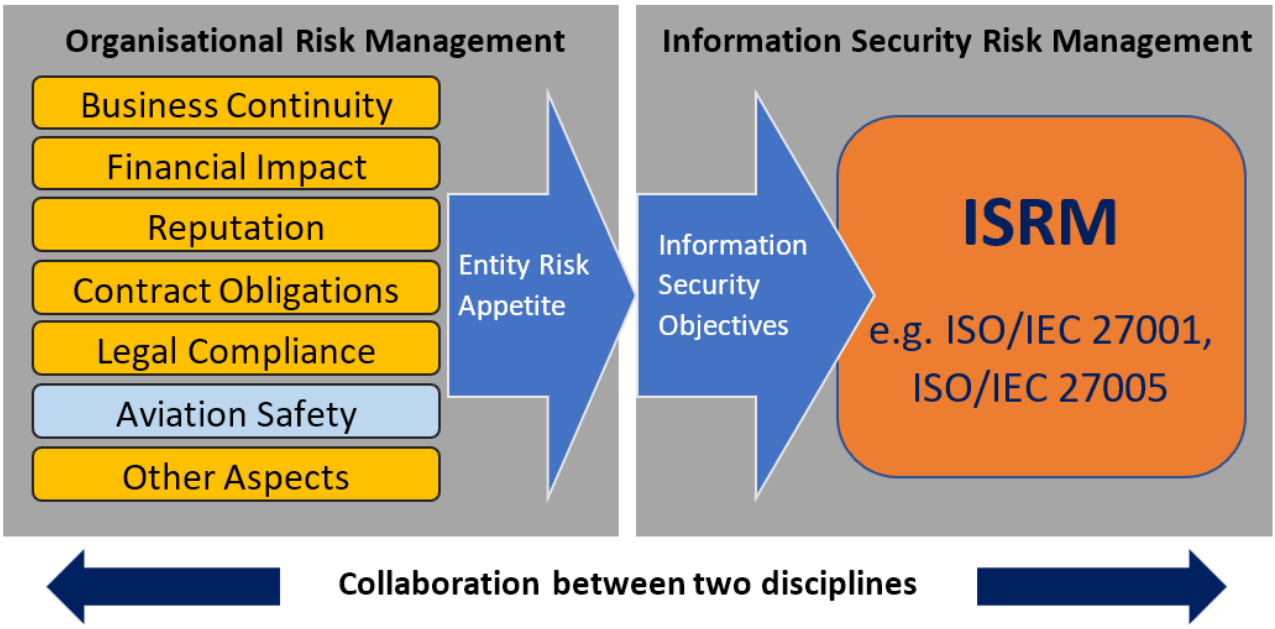
Applicability, Information Security (Part-IS)

Question:

Our organisation is ISO/IEC 27001 certified. Do I still need to comply with Part-IS?

Answer:

The requirements for an information security management system (ISMS) that are specified by Part-IS are in most parts consistent and aligned with ISO/IEC 27001; however, Part-IS introduces provisions that are specific to the context of aviation safety. If an ISO/IEC 27001-based ISMS is already operated by an entity for a different scope and context, it can be adapted and extended to the scope and context of Part-IS based on an analysis of the scope and gaps. In order to take credit from ISO/IEC 27001 certifications to achieve compliance with Part-IS, aviation safety needs to be included in the organisational risk management, with the relevant risk acceptance level determined by the applicable requirement(s) (see figure below). Moreover, for a mapping between the main tasks required under Part-IS and the clauses and associated controls in ISO/IEC 27001, refer to Appendix II of the published Acceptable Means of Compliance and Guidance Material (AMC & GM) to Part-IS.



Last updated:

05/02/2024

Link:

https://www.easa.europa.eu/en/faq/139288