European Union Aviation Safety Agency

# Risk management

## Are there examples of aviation services that may be considered when determining the information security management system (ISMS) scope and interfaces?

**Answer**

Examples of such services are provided in Appendix III to the Acceptable Means of Compliance and Guidance Material (AMC & GM) to Part-IS.

**Last updated:**
06/02/2024

**Link:**
https://www.easa.europa.eu/en/faq/139301

## Are there examples of threat scenarios that need to be considered for Part-IS?

**Answer**

A non-exhaustive list of examples of information security threat scenarios with a potential harmful impact on safety which may be considered by authorities and organisations can be found in Appendix I to the Acceptable Means of Compliance and Guidance Material (AMC & GM) to Part-IS. For further details, refer to GM IS.I.OR.205(c) or GM IS.D.OR.205(c).

**Last updated:**
06/02/2024

**Link:**
https://www.easa.europa.eu/en/faq/139302

## Is there a standard sequence to be followed when conducting an information security risk assessment?

**Answer**

Part-IS does not require the use of any specific information security risk assessment framework. Organisations can start their information security risk assessment either from the safety consequences (impact on safety) or from identifying the assets (elements) and the threats to those assets. A combination of the above methodologies is also possible and recommended.

**Last updated:**
22/08/2025

**Link:**
https://www.easa.europa.eu/en/faq/142364

## Is it acceptable to use an existing risk matrix of the organisation in order to comply with Part-IS or a new risk matrix should be designed and implemented?

**Answer**

Part-IS does not require the use of a particular risk matrix. However, it should be kept in mind that a given risk matrix is acceptable as long as it fits the purpose of properly ranking information security risks with a potential impact on safety.

**Last updated:**
22/08/2025

**Link:**
https://www.easa.europa.eu/en/faq/142365

## Is risk transfer an option under Part-IS?

**Answer**

Risk transfer is commonly associated with shifting the financial or operational consequences of a risk being shifted to a third party through insurance. In this sense, risk transfer is not a possible risk treatment option under Part-IS, since transferring responsibility to a third party (particularly an insurance company) does not imply active control of safety consequences, which is the objective of risk management in Part-IS.

Risk transfer is possible in other safety regulations, for example in the Air Operations domain. However, this is not to be confused with the risk treatment options under Part-IS, where the organisation has to take action to address identified security risks with an impact on safety.

**Last updated:**

22/08/2025

**Link:**

https://www.easa.europa.eu/en/faq/142366

## Should vulnerabilities be handled in the same way as incidents?

### Answer

Although 'vulnerability' and 'incident' are two distinct concepts, they should be handled similarly and in an integrated manner within an organisation's information security management system (ISMS). This is particularly important with regard to detection (point IS.I.OR.220(a) of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 and point IS.D.OR.220(a) of the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645), response (point IS.I.OR.220(b) and point IS.D.OR.220(b)), and reporting obligations with potential impact on aviation safety (points IS.I.OR.215 and IS.D.OR.215 as well as points IS.I.OR.230 and IS.D.OR.230).

**Last updated:**

22/08/2025

**Link:**

https://www.easa.europa.eu/en/faq/142367