# Aviation Safety within an Information Security Risk Management Process (EASA Part-IS)

2024 International Conference on Information Technologies (InfoTech-2024)

Proceedings, 11-12 September 2024, Bulgaria

Veselin Monev, PhD

# Aviation Safety within an Information Security Risk Management Process (EASA Part-IS)

**Problem**

- New EU regulations on aviation safety (EASA Part-IS) mandate convergence between aviation safety concepts and information security processes;
- The operation of an Information Security Management System (ISMS) has been mandated for aviation organisations;
- Information security risk management is a focal process that must be part of the ISMS.

**Solution**

- Integrate Part-IS requirements for risk management within an overarching Information Security Risk Management Process;
- Use a specialised risk management tool to enable efficiency and high maturity of the risk management process.

# Aviation Safety within an Information Security Risk Management Process (EASA Part-IS)

**Applicable EU regulations**

- Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022;
- Commission Implementing Regulation (EU) 2023/203 of 27 October 2022.

**Applicable requirements (controls)**

- IS.OR.205 Information security risk assessment (4 sub-groups of requirements);
- IS.D.OR.210 Information security risk treatment (3 sub-groups of requirements).

**Applicable EU guidelines**

- AMC & GM to the Articles of Regulations (EU) 2022/1645 and 2023/203;
- AMC & GM to Part-IS.AR — Issue 1;
- AMC & GM to Part-IS.D.OR — Issue 1;
- AMC & GM to Part-IS.I.OR — Issue 1.

**Other dependencies**

- Existing aviation safety risk management regulations;
- Internal policies for enterprise risk management;
- Internal policies pertaining to information security;
- ISO 27005 or NIST 800-30 for risk management.

# Aviation Safety within an Information Security Risk Management Process (EASA Part-IS)

**Key considerations of the EU regulations**

- A less stringent risk management definition compared to a typical InfoSec definition;
- Asset-oriented risk management approach is implicitly endorsed and anticipated (e.g. ISO 27005);
- Risk management process is implicit;
- Regulatory requirements should be integrated into an existing ISMS;
- A high-maturity implementation of the recommendations in the guidelines would require the utilisation of a specialised risk management tool.

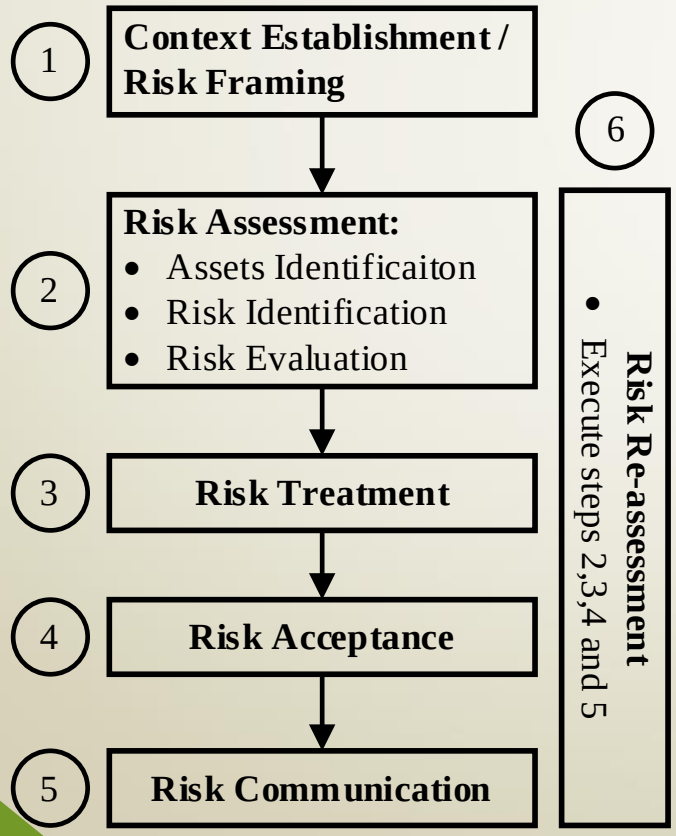
**Solution proposal**

***Implementation principles***

- Integrate regulatory requirements within an ISMS;
- Use a specialised risk management tool, such as *Governance, Risk Management, and Compliance (GRC)* tool;
- Configure the tool to auto-trigger tasks based on regulatory requirements.

# Aviation Safety within an Information Security Risk Management Process (EASA Part-IS)

## Information Security Risk Management Process




## Process implementation guidance (excerpt)

| **Requirement** |
|---|
| IS.D.OR.205 Information security risk assessment |
| **Implementation Activities** |
| Within the GRC tool:<br>• Configure automatically triggered risk assessment tasks for newly added and updated assets.<br>• Add an attribute for risk information communicated by relevant third parties.<br>• If security incidents are handled through the GRC tool, a mandatory lessons-learned field will be configured to trigger a risk re-assessment for impacted assets.<br><br>Within the documentation for risk management:<br>• An administrative (procedural) control should mandate performing a new risk assessment if the process for risk identification, risk analysis or risk classification is changed. |