SOFEMA
AVIATION SERVICES

EASA Information Security Frequently Asked Questions Review June 2025 & Supplemental Best Practice Guidance

Sofema Aviation Services Reviews the Information FAQ provided by EASA together with associated comments together with the provision of Supplemental Best Practice Guidance

To which organisations does Part-IS apply?

This Regulation applies to the following organisations (Article 2 of Regulation (EU) 2023/203):

1. maintenance organisations subject to Section A of Annex II (Part-145) to Regulation (EU) No 1321/2014, except those solely involved in the maintenance of aircraft in accordance with Annex Vb (Part-ML) to Regulation (EU) No 1321/2014;
2. continuing airworthiness management organisations (CAMOs) subject to Section A of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014, except those solely involved in the continuing airworthiness management of aircraft in accordance with Annex Vb (Part-ML) to Regulation (EU) No 1321/2014;
3. air operators subject to Annex III (Part-ORO) to Regulation (EU) No 965/2012, except those solely involved in the operation of any of the following:
    - ELA 2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012;
    - single-engine propeller-driven aeroplanes with a maximum operational passenger seating configuration (MOPSC) of 5 or less that are not classified as complex motor-powered aircraft, when taking off and landing at the same aerodrome or operating site and operating under visual flight rules (VFR) by day;
    - single-engine helicopters with an MOPSC of 5 or less that are not classified as complex motor-powered aircraft, when taking off and landing at the same aerodrome or operating site and operating under VFR by day.
4. approved training organisations (ATOs) subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011, except those solely involved in training activities of ELA2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012, or solely involved in theoretical training;

5. aircrew aero-medical centres subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011;
6. flight simulation training device (FSTD) operators subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011, except those solely involved in the operation of FSTDs for ELA2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012;
7. air traffic controller training organisations (ATCO TOs) and ATCO aero-medical centres subject to Annex III (Part ATCO.OR) to Regulation (EU) 2015/340;
8. organisations subject to Annex III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373, except the following service providers:
    - air navigation service providers holding a limited certificate in accordance with point ATM/ANS.OR.A.010 of that Annex;
    - flight information service providers declaring their activities in accordance with point ATM/ANS.OR.A.015 of that Annex;
9. U-space service providers and single common information service providers subject to Implementing Regulation (EU) 2021/664; and
10. approved organisations involved in the design or production of air traffic management/air navigation services (ATM/ANS) systems and ATM/ANS constituents subject to Implementing Regulation (EU) 2023/1769.

Moreover, this Regulation applies to the following organisations (Article 2 of Delegated Regulation (EU) 2022/1645):

1. production organisations and design organisations subject to Subparts G and J of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012, except design and production organisations that are solely involved in the design and/or production of ELA2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012; and
2. aerodrome operators and apron management service providers subject to Annex III ‘Part Organisation Requirements (Part-ADR.OR)’ to Regulation (EU) No 139/2014.

Part-IS is applicable to the competent authority responsible for the oversight of Part-66 license holders. I am a Part-66 licenced maintainer, do I also have to comply with Part-IS?

No. The rationale for requiring Part-66 competent authorities to comply with Part-IS is that there is a risk that, for example, information relating to approved Part-66 licences held by competent authorities could be compromised. This would have a potential impact on the availability and/or integrity of the information held, a risk that needs to be considered.

My organisation is not in the list of the organisations that have to comply with Part-IS but it does provide services to such organisations. Does my organisation have to comply with Part-IS?

Part-IS applies to organisations holding an approval according to any of the domain-specific regulations.

If an organisation provides services under an approval, that organisation has to comply with Part-IS requirements.

If an organisation does not hold an approval, it does not need to comply with Part-IS. However, if that organisation provides services to approved organisations, the organisation should be considered part of the functional chain to be risk-assessed as required by point IS.I.OR.205. Please refer to GM.IS.OR.205(a) for more information. Non-approved organisations must fulfill specific contractual requirements agreed with the (approved) organisation that has to comply with Part-IS. Please refer to GM1 IS.OR.205(b) for more information.

My organisation holds an EASA Part-145 approval under a Bilateral Agreement with the European Community. Does Part-IS apply in such case?

Under a Bilateral Agreement, the applicability of EASA regulations, including Part-IS, might be subject to the terms of that agreement. Bilateral Agreements often include provisions for mutual recognition of certain certification standards, but they may not automatically include all aspects of EASA regulations like Part-IS.

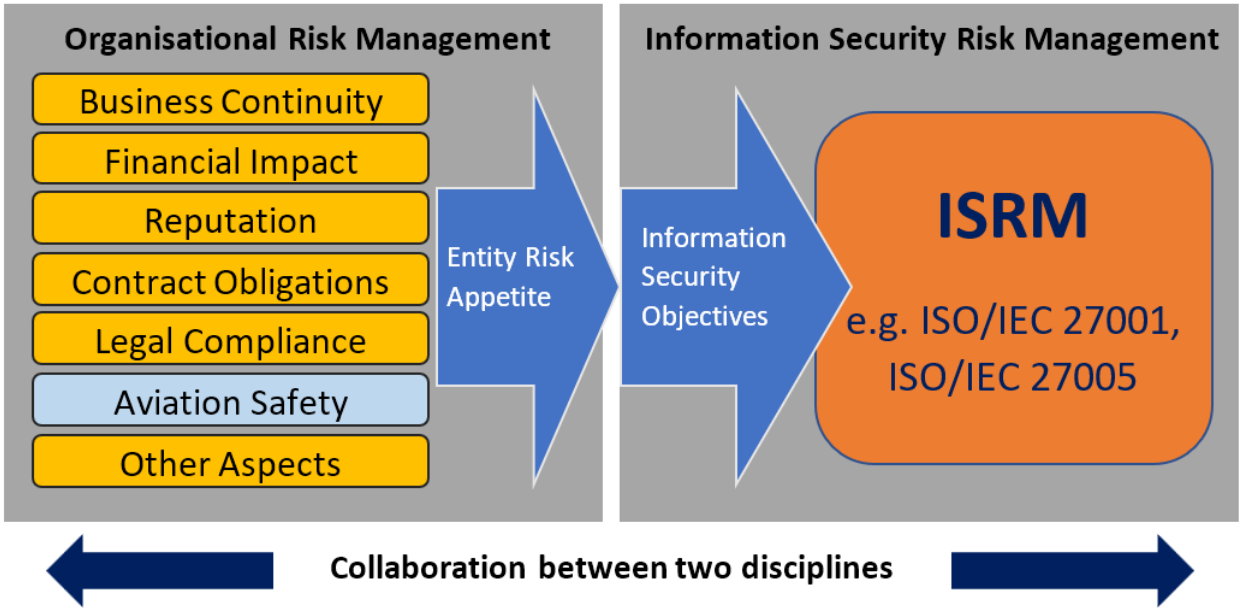
To determine whether Part-IS applies to your organization under the Bilateral Agreement, you should review the specific terms of the Bilateral Agreement to understand which EASA regulations are recognised and applicable.

My organisation is an operator or entity referred to in the national civil aviation security programmes of Member States laid down in accordance with Article 10 of Regulation (EC) No 300/2008 and complies with the cybersecurity requirements of point 1.7 of the Annex to Implementing Regulation (EU) 2015/1998. As a consequence, is the organisation considered to be fully compliant with Part-IS?

No, as required by Article 4(2) of Delegated Regulation (EU) 2022/1645 and Article 5(2) of Implementing Regulation (EU) 2023/203 and in addition to those requirements, point IS.OR.230 needs to be complied with in order to have legal compliance with the requirements stemming from Part-IS. Compliance with Part-IS will be verified by the competent authority that is identified in Article 6 of the Implementing Regulation and Article 5 of the Delegated Regulation.

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

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.



My organisation has to comply with Directive (EU) 2022/2555 (the 'NIS 2 Directive'). Does it also have to comply with Part-IS or is it considered covered?

According to the Guidelines provided by the European Commission on 'sector-specific Union legal acts', Part-IS does not fall under the category of 'Lex Specialis' (refer to Article 4 of the NIS 2 Directive). This is mainly due to the specific scope of the information security management system (ISMS) legislation as compared to the broader approach of the NIS 2 Directive. However, EASA is working with the European Commission to have Part-IS compliance 'credited' in the context of NIS 2 compliance. This can be achieved either during the incorporation of the Directive into national legislation or during the implementation phase. Further guidance on this topic will be provided in 2025.

Article 5(1) of Implementing Regulation (EU) 2023/203 and Article 4(1) of Delegated Regulation (EU) 2022/1645 refer to the equivalence of requirements between Directive (EU) 2016/1148 (NIS Directive) and Part-IS. Does this mean that if one complies with the NIS Directive or the NIS 2 Directive, they are automatically compliant with Part-IS?

No. Compliance with NIS requirements does not imply compliance with all Part-IS requirements. Compliance with the security requirements of Article 14 of Directive 2016/1148 (the 'NIS Directive') or Article 21 of Directive (EU) 2022/2555 (the 'NIS 2 Directive') must be equivalent in effect with the corresponding requirements of Part-IS.OR. This equivalence in effect with Part-IS will be verified by the competent authority that is identified in Article 6 of Implementing Regulation (EU) 2023/203 and Article 5 of Delegated Regulation (EU) 2022/1645.

Article 5(1) of Implementing Regulation (EU) 2023/203 and Article 4(1) of Delegated Regulation (EU) 2022/1645 refer to Directive (EU) 2016/1148 (the 'NIS Directive') and its relation to Part-IS. As Directive (EU) 2022/2555 (the 'NIS 2 Directive') will be applicable from October 2024, does this means that automatically any references to the 'old' NIS Directive in Part-IS refer now to the NIS 2 Directive?

Yes, according to Article 44 of Directive (EU) 2022/2555 (the 'NIS 2 Directive'):

'Directive (EU) 2016/1148 is repealed with effect from 18 October 2024.

References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex III.'

As the 'Authority Requirements' are part of Implementing Regulation (EU) 2023/203, which is applicable from 22 February 2026, does this mean that the

applicability date (16 October 2025) of Delegated Regulation (EU) 2022/1645 can be then entirely disregarded?

Regulatory deadlines cannot be disregarded. Therefore, organisations within the scope of Delegated Regulation (EU) 2022/1645 have to comply with it by 16 October 2025. However, as the 'Authority Requirements' (of Implementing Regulation (EU) 2023/203) will only be applicable as of 22 February 2026, it is possible that before that date, National Aviation Authorities (NAAs) might not be fully compliant with those Authority Requirements. NAAs must nevertheless enforce the Delegated Regulation during the four months between the two applicability dates as an oversight obligation stemming from Article 62 of Regulation (EU) 2018/1139 (the 'Basic Regulation'). However, a lenient approach is advised to be followed until the Implementing Regulation becomes applicable.

At the same time, we would recommend that all affected parties, i.e. authorities and organisations, incorporate Part-IS into their processes as early as possible, as the objective is to ensure adequate protection of the aviation ecosystem and not merely compliance.

Does information have to be protected only from digital threats or also from non-digital ones?

The use of the term 'information security' in Part-IS, as opposed to 'cybersecurity', is deliberate and significant. This terminology is chosen to encompass a broader range of risks associated with information systems. Unlike 'cybersecurity', which primarily focuses on protecting data from digital threats in cyberspace, 'information security' is extended beyond the digital realm to include analogue threats. This comprehensive approach acknowledges that vulnerabilities and threats to information systems can arise in both digital and physical formats, thereby necessitating a wider scope of protective measures and considerations.

Derogation

My organisation would like to apply for a derogation. Is it eligible and if so, what procedure should be followed?

As per GM1 IS.D.OR.200(e):

'Any organisation that believes that it does not pose any information security risk with a potential impact on aviation safety, either to itself or to other organisations, may consider requesting an approval for a derogation by the competent authority by

performing a documented information security risk assessment following the procedure outlined in AMC1 IS.D.OR.200(e).'

Indicatively, such organisations might include design organisation approval (DOA) or production organisation approval (POA) holders that design or produce only components or parts that either are not involved in ensuring the structural integrity of the aircraft (e.g., carpets, interiors) or have no major safety-related aircraft functionalities, including but not limited to, aircraft software, navigation, avionics, engines, flight control, landing gear, hydraulic, electrical, air, communications, etc..

The aforementioned example is only indicative of what could provide an initial basis for the preparation of an information security risk assessment that justifies the exclusion of all elements of an organisation from the scope of the information security management system (ISMS). It is up to the authority to determine whether the assessment provided by the organisation is deemed satisfactory for a derogation to be granted.

If my organisation receives a derogation, does this mean that it is exempted from compliance with Part IS?

A derogation is a temporary exemption from the full requirements of a regulation. The organisation is advised to remain vigilant and, as a minimum, reassess its exposure to cybersecurity threats whenever the scope changes. In particular, the continued validity of that derogation will be reviewed by the competent authority following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.

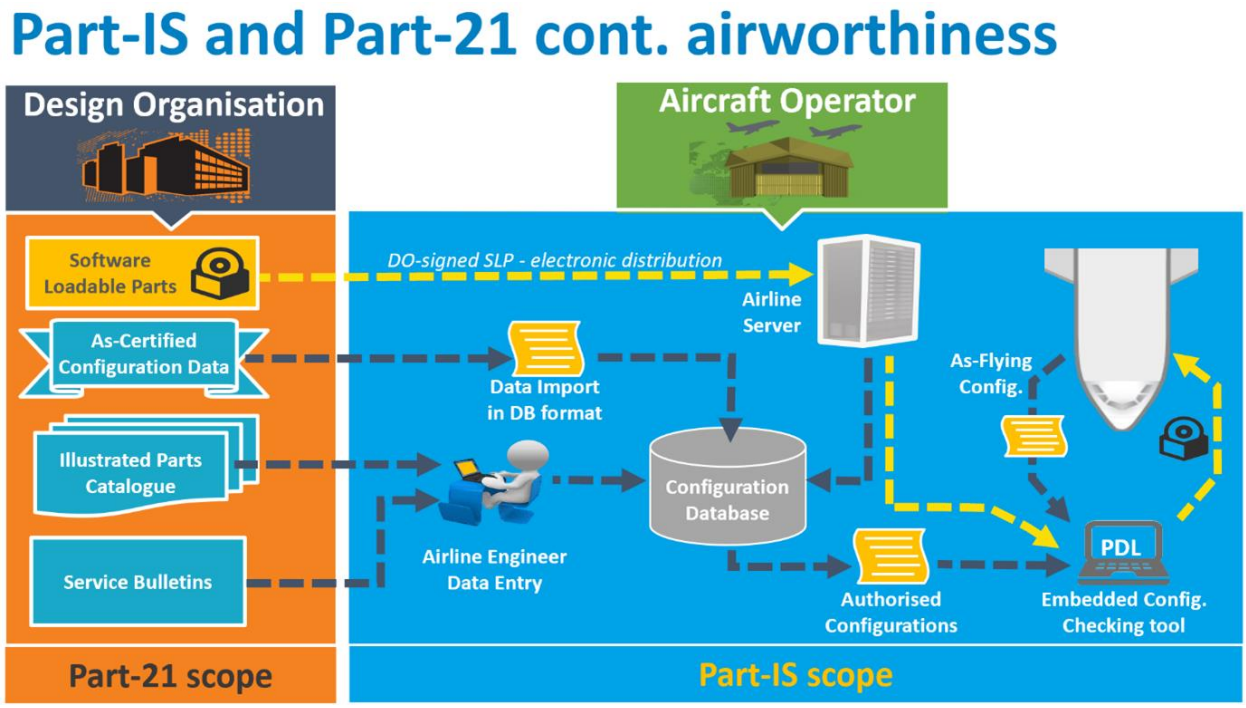
Relationship between Part-IS and certified products

What is the relationship between product and organisation information security, for example, how does an aircraft certified under CS 25.1319 fits in Part-IS?

Part-IS is a set of rules that aims to address information security risks at the entity level by establishing processes to ensure the protection of all elements identified as part of its scope. In order to identify which elements (and relevant assets) of an entity may be exposed to information security risks and therefore need to be included in the scope of Part-IS, an information security risk assessment shall be carried out in accordance with point IS.OR.205.

Aeronautical products, such as an aircraft whose certification includes airworthiness security objectives, will be important elements to be considered in the scope of Part-IS, for example, for an air operator. Any procedures already in place for meeting the

requirements arising from the product certification will need to be complemented by the new organisational requirements under Part-IS to ensure a holistic protection of all identified assets and of their interfaces with other elements and organisations. Below is a graphic illustration of an example of the scope and interaction between Part-IS and Part-21 in relation to continuing airworthiness activities.



What tool should be used to report information security incidents?

Reporting obligations under point IS.OR.230(b) and Regulation (EU) No 376/2014 (the 'Occurrence Reporting Regulation') may be discharged using one reporting channel. Currently, EASA is assessing ECCAIRS-2 and envisaging to update its taxonomy and processes to make it more compatible for possible future reporting of information security incidents.

Delegation of tasks

An organisation holds multiple approvals or declarations. Can the different accountable managers delegate the activities under Part-IS to a single person?

Yes, when the organisation shares information security organisational structures, policies, processes and procedures with other organisations or with areas of their own

organisation that are not part of the approval or declaration, the accountable manager may delegate their activities to a common responsible person.

Coordination measures shall be established between the accountable manager, or accountable managers for those entities holding multiple approvals, and the common responsible person to ensure adequate integration of the information security management within the organisation(s).

Does the organisation need to establish a separate representative for the information security management system (ISMS)?

This is an organisational decision depending on the necessary competencies that this person needs to have. The accountable manager may decide to delegate certain responsibilities to a person or group of persons, taking into account their competencies and the requirements detailed in point IS.OR.240 and the related acceptable means of compliance and guidance material (AMC & GM).

Competencies

What are the necessary competencies that will need to be developed in order to comply with Part-IS?

In order to develop the list of competencies, an organisation may use, as initial guidance, an existing cybersecurity competency framework such as the National Initiative for Cybersecurity Education (NICE) based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

In Appendix II to the published Acceptable Means of Compliance and Guidance Material (AMC & GM) to Part-IS, the main tasks of Part-IS are listed and mapped to the competencies derived from the NIST CSF. More information may be found in the AMC & GM to Part-IS. Moreover, entities may utilise the material of the European Cybersecurity Skills Framework (ECSF) that is published by ENISA. EASA has therefore produced a document with the objective of providing a high-level case study of the application of the ECSF in aviation for the implementation of Part-IS.

More information and the actual document may be found here.

Risk assessment

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

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

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

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. Please also refer to GM IS.I.OR.205(c) or GM IS.D.OR.205(c) for further details.

Integration into existing management systems

Can the Part-IS information security management system (ISMS) requirements be integrated into existing management systems?

It is possible to include the ISMS requirements in an overarching management system comprising information security, aviation safety, quality management etc. Moreover, as explained in further detail in FAQ n.139288, already existing ISMSs (e.g., from ISO/IEC 27001) can be tailored to the needs of Part-IS. From an organisational perspective, different types of risks interact with each other, and the implementation of certain controls (measures) may address more than one type of risks. Interacting bow ties allow for a higher-level and non-exhaustive illustration of how different disciplines of risk assessment may need to collaborate to establish a common risk perspective, as depicted in Figure 1 below:

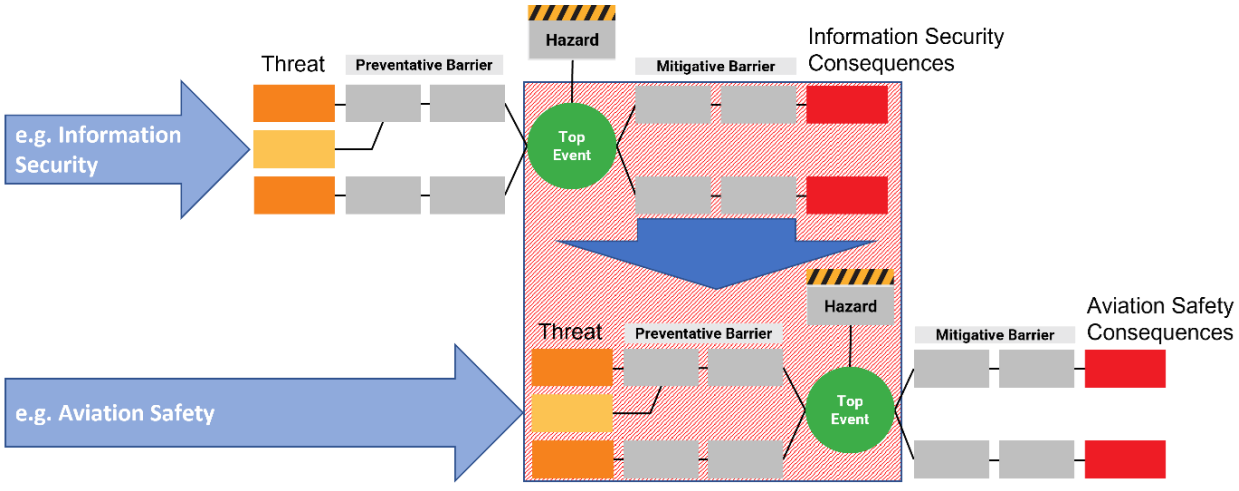
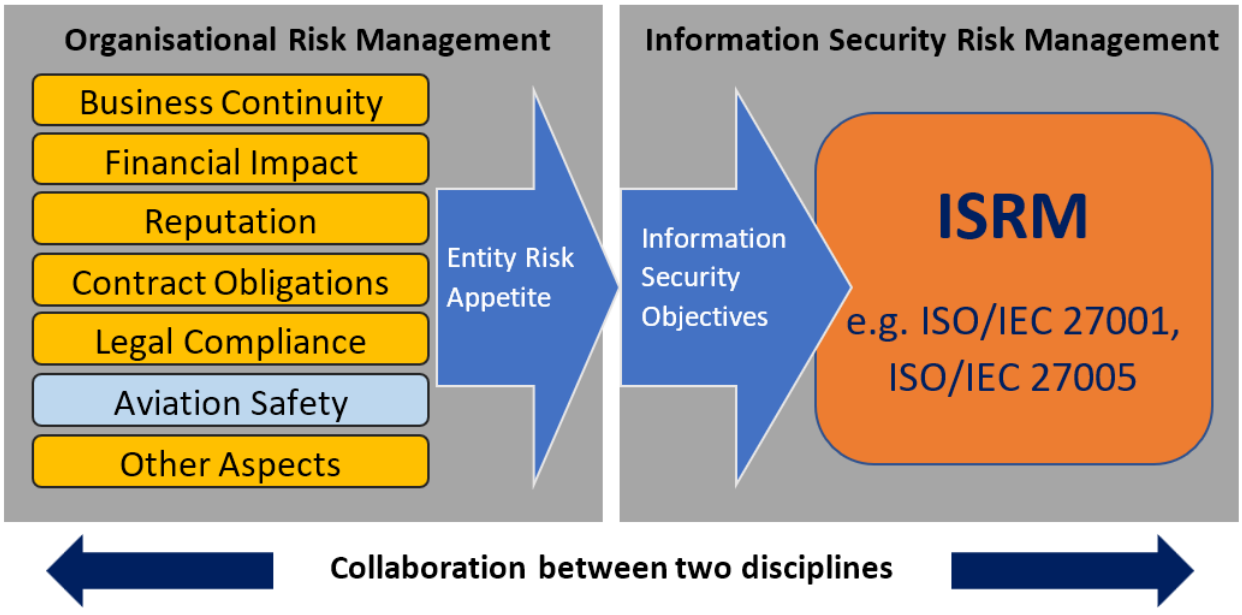


Figure 1 — Bow-tie representation of management of aviation safety risks posed by information security (IS) threats

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.



Supplementary material

Are the standards referenced in the Acceptable Means of Compliance and Guidance Material (AMC & GM) to Part-IS for free or to be purchased?

The standards referenced in the AMC & GM to Part-IS are publicly available. However, as with any standard, their content is subject to intellectual property rights (IPRs), i.e., those standards are the exclusive intellectual and commercial property of the standardisation organisation that produced and published them. As such, the AMC & GM to Part-IS can only refer to them, and in most cases, the standards have to be purchased by interested organisations.

Supplemental Best Practice Guidance for Implementing EASA Part-IS Information Security Requirements

Introduction - This document supports aviation organisations in applying the requirements of EASA Part-IS. While the FAQ provides clarity on regulatory expectations, this guide offers practical best practices for effective implementation. The aim is to promote a proactive security posture, build resilience across the aviation ecosystem, and ensure seamless integration with existing management systems.

Applicability and Scoping - Best Practice:

- Conduct a **comprehensive applicability review**: Ensure the organisation understands whether it falls under mandatory compliance or must be risk-assessed as part of a contractual relationship (per IS.I.OR.205).
- Perform a **gap analysis** if already ISO/IEC 27001 certified: Map your current ISMS scope to aviation safety exposure and adjust risk thresholds accordingly.
- **Maintain a dynamic scope document** for your ISMS that evolves with changes in service portfolio, technology, or partnerships.

Risk Assessment and Asset Mapping - Best Practice:

- Apply a structured framework such as **NIST CSF** or **ENISA ECSF** to define and manage risk.
- Document all **information assets and dependencies**, including third-party services, cloud infrastructure, software tools, and operational interfaces.
- Integrate threat modeling using **scenarios from Appendix I** of the AMC & GM to Part-IS to inform mitigation strategies.

Third-Party and Supply Chain Considerations - Best Practice:

- For non-approved service providers, create **detailed contractual clauses** addressing security obligations and audit rights.

- Use a **tiered risk model** to assess subcontractor exposure and enforce compliance measures proportionate to their integration with your ISMS.

Integration with Existing Management Systems - Best Practice:

- Leverage synergies with Safety Management Systems (SMS), Quality Management (e.g., ISO 9001), and Environment (e.g., ISO 14001) by building a **Unified Risk Governance Model**.
- Consider developing a **"Risk Register Matrix"** that cross-references safety, quality, and information security threats, supported by bow-tie analysis.

Derogation Considerations - Best Practice:

- When seeking a derogation, ensure the **risk assessment is robust and evidence-based**, clearly showing no adverse impact on aviation safety.
- Implement a **continuous monitoring mechanism** to reassess eligibility should the organisation's scope evolve.

Competence Development - Best Practice:

- Develop a **training and competence matrix** aligned with ECSF and NIST roles such as Risk Analyst, Security Architect, Incident Handler.
- Assign **role-specific ISMS responsibilities** and validate knowledge through regular simulation-based exercises and refresher training.

ISMS Governance Structure - Best Practice:

- Designate a **single ISMS Representative** to ensure coherence across departments and approvals, even in multi-entity structures.
- Ensure the **Accountable Manager formally endorses** the ISMS policy and is regularly briefed on its status and performance metrics.

Reporting and Continuous Improvement - Best Practice:

- Establish **clear internal escalation protocols** for IS-related incidents and train staff to recognise early indicators.
- Use the **ECCAIRS-2 platform** or any updated EASA-endorsed reporting tools once harmonised for information security events.
- Perform **post-incident reviews** and adapt the ISMS to reflect lessons learned.

Harmonisation with Other Frameworks - Best Practice:

- Where compliance with **NIS 2 Directive** is also mandated, maintain a **cross-regulation compliance matrix** to avoid duplication and demonstrate equivalence in controls.
- Actively monitor **Member State interpretations** of NIS 2 to determine how Part-IS implementation may support national requirements.

Documentation and Records Management - Best Practice:

- Maintain detailed records of:
    - Scope definition
    - Risk assessments
    - Training records
    - Incident logs
    - Audit findings
    - Compliance declarations
- Ensure documentation is **readily accessible** and aligns with audit and oversight requirements of the National Aviation Authority (NAA).

Cultural and Organisational Resilience - Best Practice:

- Promote a **security-first culture** by embedding information protection into daily operations.
- Conduct **awareness campaigns** to enhance employee vigilance against phishing, social engineering, and insider threats.

Timeline for Implementation - Organisations must achieve compliance with **Delegated Regulation (EU) 2022/1645** by **16 October 2025**. Full **authority oversight obligations** under Implementing Regulation (EU) 2023/203 apply from **22 February 2026**. Early adoption and internal audits are encouraged to facilitate smooth transition and regulator engagement.

Final Recommendation - The goal of Part-IS is not only compliance but to foster a **robust and resilient aviation ecosystem** that protects critical information assets from both digital and analogue threats. Organisations are encouraged to implement a **mature**

ISMS, engage with stakeholders across the operational chain, and continuously evolve their security practices in line with emerging threats and technologies.