European Union Aviation Safety Agency

Information Security (Part-IS)

Applicability

To which organisations does Part-IS apply?

Answer

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; organisations satisfying both exceptions are also exempted.
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.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/139283

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?

Answer

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.

Last updated:
05/02/2024

Link:
https://www.easa.europa.eu/pt/faq/139284

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

Answer

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.

Last updated:
22/01/2024

Link:
https://www.easa.europa.eu/pt/faq/139286

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?

Answer

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.

Last updated:

05/02/2024

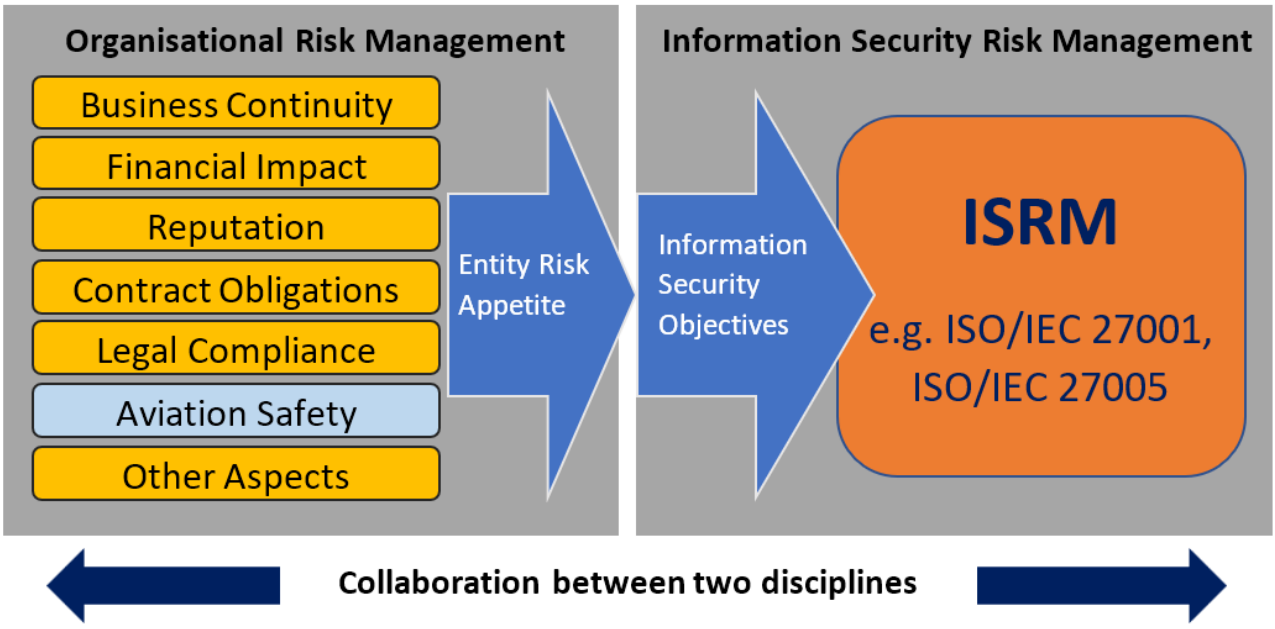
Link:

https://www.easa.europa.eu/pt/faq/139287

My 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:

Last updated:
21/08/2025

Link:
https://www.easa.europa.eu/pt/faq/139288

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?

Answer

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.

Last updated:
10/12/2024

Link:
https://www.easa.europa.eu/pt/faq/139289

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?

Answer

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. Supporting material for performing this assessment is currently under development by the European Commission, the European Union Aviation Safety Agency (EASA), and the Member States' authorities, and is expected to be provided to the authorities concerned by 2025/Q4.

Last updated:

22/08/2025

Link:

https://www.easa.europa.eu/pt/faq/139290

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?

Answer

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.'

Last updated:

05/02/2024

Link:

https://www.easa.europa.eu/pt/faq/139291

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 disregarded?

Answer

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 will only be applicable as of 22 February 2026, it is possible that before that date Competent Aviation Authorities (CAAs) might not be fully in compliance with the Authority Requirements. National Aviation Authorities (NAAs) have nevertheless to enforce the Delegated Regulation during the four months between the two applicability dates as an oversight obligation stemming from Article 62 of the Basic Regulation. However, a lenient approach is advised to be followed until the Implementing Regulation becomes applicable.
More information on guidelines on the oversight approach by the authorities

At the same time, we would recommend that all affected parties, authorities, and organisations integrate 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.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/139292

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

Answer

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.

Last updated:
05/02/2024

Link:
https://www.easa.europa.eu/pt/faq/139293

Why are there two sets of rules (Implementing Regulation and Delegated Regulation), and what is the difference between them?

Answer

Further to the changes introduced in the EU legislative process by the Lisbon Treaty, the European Commission has been given the power to adopt delegated acts in certain areas following a simpler and faster process. In all other cases, the adoption of implementing acts requires to follow the Comitology process, which includes a vote by Member States.

According to Article 128 of the Basic Regulation, the European Commission has been given the power to adopt delegated acts in the areas of Initial Airworthiness and Aerodromes.

For this reason, two acts have been issued to introduce Part-IS requirements: Delegated Regulation (EU) 2022/1645 and Implementing Regulation (EU) 2023/203. Their applicability scope reflects the delegations conferred in Article 128 of the Basic Regulation.

The two acts were scheduled to be issued simultaneously, but issues during the publication process led to a delay of the publication of the Implementing Regulation and, consequently, to the staggered applicability dates.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142353

Is Part-IS applicable to Declared Organisations, and if so, to which Declared Organisations?

Answer

The following Declared Organisations have to comply with Part-IS requirements:

1. Non-Commercial Operations with Complex Aeroplanes (NCC) Organisations — Air Operations (Air OPS),
2. Specialised Operations (SPO) Organisations — Air OPS,
3. Apron Management Service Providers — Aerodromes (ADR), and
4. Ground Handling Service Providers.

The following Declared Organisations are out of scope and do not have to comply with Part-IS requirements:

1. Declared Training Organisations (DTOs) — Aircrew.
2. Part-ML (Light) Organisations, and
3. Declared Design Organisation Approval (DOA) Holders.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142354

How is Part-IS applied and its application overseen in organisations under a declaratory regime (i.e. Declared Organisations, where no approval in advance is required)?

Answer

Given their status, Declared Organisations (DOs) shall not seek approval in advance of their information security management manual (ISMM) and of their procedure for management of changes. Delegated Regulation (EU) 2022/1645 has been amended by Delegated Regulation (EU) 2025/22, while the amendment of Implementing Regulation (EU) 2023/203 is currently pending. For more details on DOs and their oversight regime, please refer to Subpart DEC of Annex III (Part-ORO) to Regulation (EU) No 965/2012 (Air OPS Regulation).

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142355

If the Member State decides to designate another entity to fulfil the assigned role and responsibilities of the competent authority according to Article 6(2) of Implementing Regulation (EU) 2023/203, which authority will Annex I (Part-IS.AR) to that Regulation apply to? To the designated entity or to the competent authority identified in Article 6(1)?

Answer

The applicability of Part-IS.AR (authority requirements) is specified in the implementing rules for each specific domain under the relevant authority requirements (e.g. for authorities designated in accordance with Annex II (Part-145) to Commission Regulation (EU) No 1321/2014, see point 145.B.200). This applicability has been introduced by means of an amendment to the already existing authority requirements for the establishment of a management system. Therefore, these requirements apply regardless of how roles and responsibilities are allocated

to an independent and autonomous entity designated by the Member State under Article 6(2) of Part-IS.AR.

At the same time, there are no provisions for the implementation of an ISMS derived from Part-IS that apply to the independent and autonomous entity designated by the State in accordance with Art. 6.2 of Part-IS.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142356

If the competent authority identified in Article 6(1) of Implementing Regulation (EU) 2023/203 decides to allocate certain tasks related to oversight under Part-IS to a qualified entity, which entity has to comply with Part-IS?

Answer

Delegation to a qualified entity refers to specific oversight tasks resulting from the authority requirements (e.g. for authorities designated in accordance with Annex II (Part-145) to Commission Regulation (EU) No 1321/2014, see point 145.B.205). The authority requirements of Part-IS shall be met by the competent authority designated in the implementing rule for the domain (which is identical to the one referred to in Article 6(1), if the delegation under Article 6(2) is not exercised by the Member State).

Where the competent authority delegates certification or oversight tasks, its information security management manual (ISMM) shall also cover the activity delegated to the qualified entity (e.g. for Part-145, see point 145.B.205(c)(3)).

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142358

Does the ELA2 exemption cover also ELA1 aircraft?

Answer

ELA1 aircraft fall below the ELA2 threshold; therefore, organisations dealing only with

ELA1/ELA2 aircraft are also exempted from complying with the Part-IS requirements.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142359

A production organisation under Annex I (Part-21), Subpart G to Commission Regulation (EU) No 748/2012 approval designs and manufactures parts for ELA1/ELA2 aircraft. Is the ELA2 exemption applicable to that organisation if it can clearly demonstrate that it is exclusively involved in the development and/or production of ELA1 or ELA2 aircraft, or is the exemption limited to the aircraft manufacturer?

Answer

The exemption contained in Article 2(1) of Delegated Regulation (EU) 2022/1645 only refers to Design or Production Organisations (DPOs) that are solely involved in the design and/or production of ELA2 aircraft. DPOs designing and/or producing parts to be installed in this category of aircraft are not included in the exemption.

Further to a risk assessment, it is possible for such organisations to ask for a derogation in accordance with point IS.D.OR.200(e) of Annex II (PART-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142360

Do TCO operators have to comply with Part-IS?

Answer

The operator as such (the AOC holder) does not have to comply with Part-IS. However, if that airline holds other EASA certificates for their maintenance (Part-145) or training (ATO or FSTD) branch, then Part-IS is applicable to the part of the organisation covered by such certificates.

Last updated:

30/09/2025

Link:
https://www.easa.europa.eu/pt/faq/142526

Derogation

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

Answer

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. More information on the derogation process.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/139294

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

Answer

A derogation is a temporary exemption from the full requirements of the 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 approval 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.

There are a few requirements that still apply or partially apply to a derogated organisation. More information on this and the derogation process.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/139295

Is the derogation provision under point IS.D.OR.200(e) or point IS.I.OR.200(e) linked to the flexibility provisions of Article 71 of the Basic Regulation?

Answer

Point IS.D.OR.200(e) of the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645 or IS.I.OR.200(e) of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 provide for a self-contained derogation possibility which can be used independently of Article 71. Those points allow an organisation to be temporarily exempted from implementing an information security management system, provided that its activities, facilities, resources, and services do not pose any information security risks that could affect aviation safety. Therefore, the two are not linked.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142361

Relationship between Part-IS and certified products

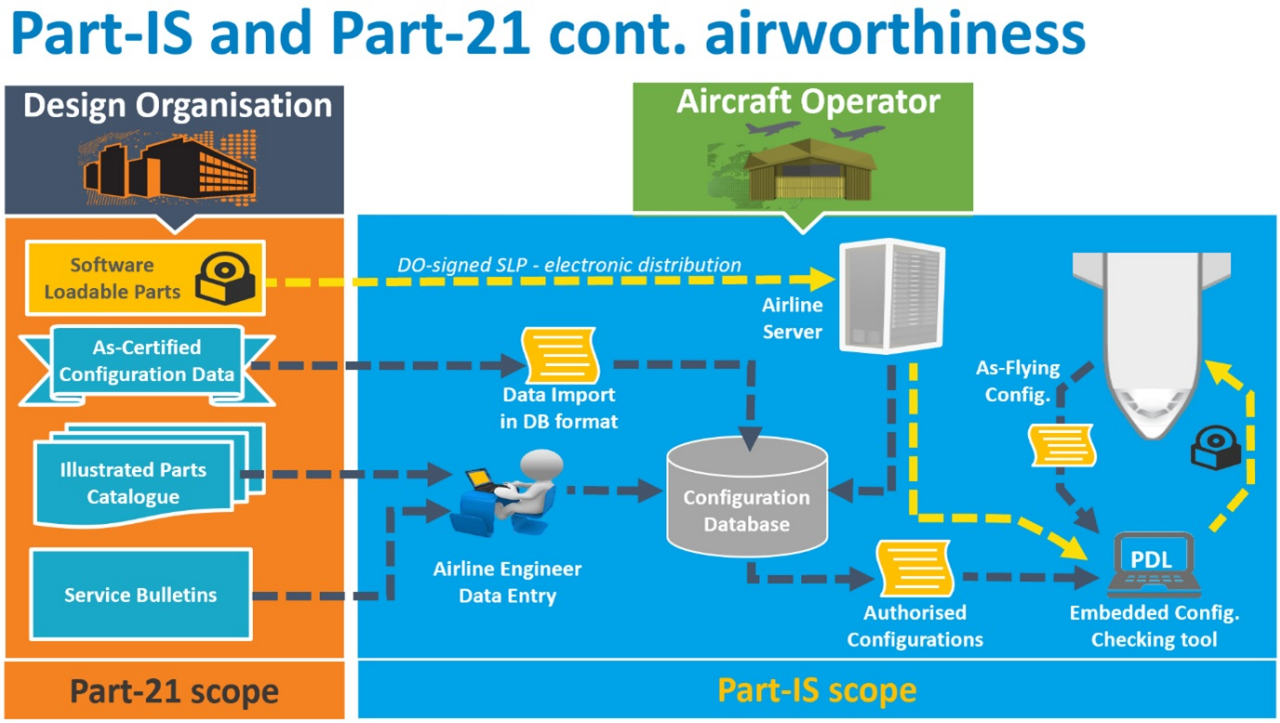
What is the relationship between product and organisation information security, for example, how does an aircraft certified under CS 25.1319 fit in

Part-IS?

Answer

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 of the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645.

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 Annex I (Part 21) to Commission Regulation (EU) No 748/2012 in relation to continuing airworthiness activities.



Last updated:

22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/139296

Reporting

What tool should be used to report information security incidents?

Answer

In Part-IS, the requirements for internal reporting (point IS.I.OR.215 (a) and (b) of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 and point IS.D.OR.215 (a) and (b) of the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645) and for external reporting (point IS.I.OR.230 (a) and (b) of Part-IS.I.OR and point IS.D.OR.215 (a) and (b) of Part-IS.D.OR) do not specify a particular reporting tool, leaving this at the discretion of the organisations. However, according to point IS.OR.230(a) and Article 7 of Regulation (EU) No 376/2014 (Occurrence Reporting), to facilitate information exchange, occurrence reports should be stored in databases which should be compatible with the ECCAIRS-2, the EASA/European Commission reporting tool.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/139297

Governance

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

Answer

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).

Last updated:
06/02/2024

Link:
https://www.easa.europa.eu/pt/faq/139298

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

Answer

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.I.OR.240 of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 and point IS.D.OR.240 of the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645 as well as in the related acceptable means of compliance and guidance material (AMC & GM).

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/139299

Should an organisation have one single information security policy even if there are different organisation approvals (OAs) under its umbrella?

Answer

An organisation is free to choose to have a single information security policy covering all OAs or a different information security policy per OA.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142362

Competencies

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

Answer

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.

Last updated:
06/02/2024

Link:
https://www.easa.europa.eu/pt/faq/139300

How to assess competence when using the provisions of IS.I.OR.235 of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 or point IS.D.OR.235 of the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645 to subcontract information security activities when the organisation does not have the necessary knowledge?

Answer

Documentation of qualifications can be used in this regard as well as the experience (track of records, customers) of the organisation providing the services. For more information, see FAQ n.139300.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142363

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/pt/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/pt/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/pt/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/pt/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/pt/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/pt/faq/142367

Supply chain

Does Part-IS have requirements on suppliers/subcontractors that although they are not within the list of the organisations that have to comply with Part-IS, they work with/for an organisation that is within the Part-IS scope?

Answer

Part-IS requirements are addressed to organisations within the scope of the rules (Article 2 'Scope' of Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation (EU) 2022/1645). These organisations need to address the information security risks at the interfaces with other organisations, whether the latter are within or outside the scope of the rule. To do so, organisations within the scope have two options:

1. they can either implement mitigation measures and controls within their own organisational boundaries; or

2. they may decide instead to manage the risks through contractual agreements and require the supplier/subcontractor to implement mitigation measures and controls within its own organisation.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142368

Is IS.I.OR.235 applicable to all suppliers/subcontractors?

Answer

No. The requirement of point IS.I.OR.235 of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 is applicable only to those suppliers/subcontractors that perform tasks pertinent to information security management activities. All the rest are covered by point IS.I.OR.205 to Part-IS.I.OR.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142369

Can Part-IS implementation and/or the Part-IS compliance monitoring function be subcontracted? If yes, is the subcontracted organisation responsible for implementation and compliance?

Answer

Yes, Part-IS implementation and/or its compliance monitoring function can be subcontracted. It is important to note that the responsibility for performing tasks pertinent to Part-IS can be transferred, accountability however cannot. The organisation subject to Part-IS is always accountable for the implementation of the rule and for demonstration of compliance to the rule. This should be clarified in the agreement between the organisation subject to Part-IS and the subcontractor.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142370

Integration into existing management systems

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

Answer

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:

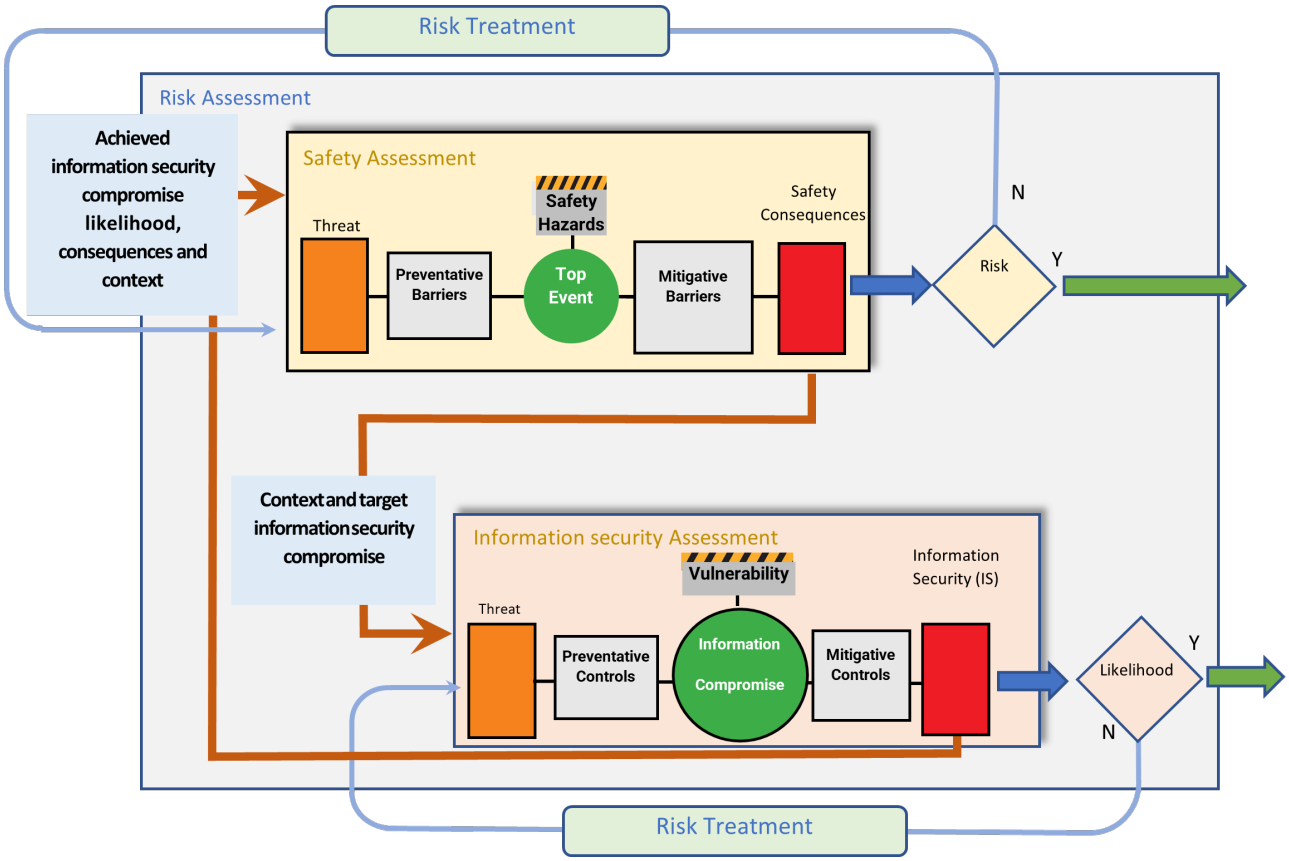


Figure 1 — Bow-tie representation of management of aviation safety risks posed by information security (IS) threats

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/139303

Documentation

Does the information security management manual (ISMM) have to be a single document containing all the information required, or can it be a set of separate documents covering the topic specified under point IS.I.OR.250(a) of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 or point IS.D.OR.250(a) of the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645?

Answer

Several formats can be used for the ISMM. It can be a standalone manual or it can be integrated into an existing manual/exposition. Alternatively, it can be a slim document with a skeleton that directs readers to separate documents. In any case, there is a need to have clear identifiers for the manual, its approvers, and its revisions.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142371

Can the term "archived" in point IS.I.OR.245 of Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 or point IS.D.OR.245 of the Annex (Part-IS.D.OR) to Commission Delegated Regulation (EU) 2022/1645 be understood as "archiving" as described in the EN9130 standard?

Answer

No. Under the EN9130 standard, archiving is the “process of moving one or more electronic record extracts to off-line storage in a way that ensures the possibility of restoring them to on-

line storage when needed without loss of meaning. Wherever possible, archived data should be technology-independent so that future users do not have dependencies on obsolete technology from the past".

In the context of Part-IS, archiving should be understood as "stored in a manner that ensures protection from damage, alteration and theft, with information being identified, when required, according to its security classification level". Moreover, integrity, authenticity, and authorised access shall be ensured (refer to point IS.I.OR.245(d) of Part-IS.I.OR or point IS.D.OR.245(d) of Part-IS.D.OR).

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142372

Oversight approach

What is expected by organisations by the applicability date of the regulation?

Answer

The implementation of Part-IS is not a binary process, but rather a continuous one with different implementation levels to be achieved. Organisations are expected to follow the PSOE (Present, Suitable, Operational, Effective) model and be under the 'Present' and 'Suitable' levels by the applicability date.

This is a notion familiar to the organisations applying already a safety management system (SMS). In short, the organisations need:

- to establish the fundamental elements of the information security management system (ISMS);
- to define the personnel roles and responsibilities as well as the scope; and
- to define a security policy, a risk management process as well as change management policies.

Moreover, procedures on incident management and reporting (internal) of events are expected to set the stage for formalising security management. Following this, the organisation should further proceed in terms of implementation levels, reaching the 'Operational' and 'Effective' levels.

More information on guidelines on the oversight approach by authorities

Last updated:

22/08/2025

Link:

https://www.easa.europa.eu/pt/faq/142374

When acting as competent authority, what is EASA's policy for Part IS oversight while organisations are in the process to achieve the operational Part IS implementation stage?

Answer

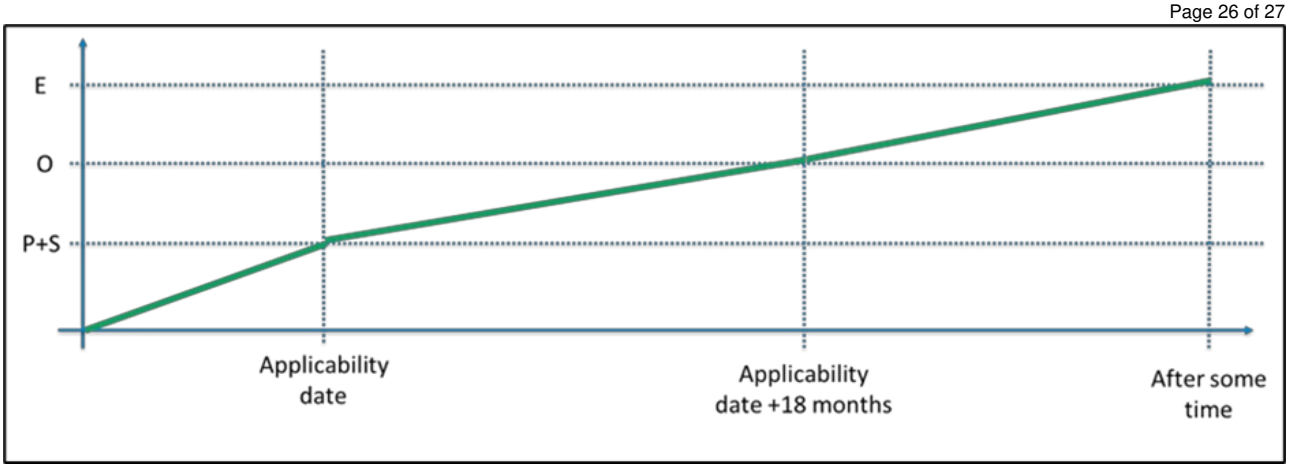
The general implementation principles are outlined in the Guidelines for Part-IS oversight approach jointly developed by Member State authorities and EASA in the Part-IS Implementation Task Force.

To further precise the above guidance EASA in its role as competent authority, e.g. for organisations outside the EU MS, has developed further implementation guidance documents. These documents are based on the following principles:

EASA has decided to allow organisations under its responsibility an 18 month development phase for the full implementation of Part IS, i.e. it is acknowledged that organisations will need this time to develop their Information Security Management System from a present and suitable to a full operational level (the PSOE model is used here in analogy to the SMS implementation levels for clarity/simplification).

The overseen organisations should make best use of this development period to progress towards the operational level of implementation. In line with the published implementation guidelines, EASA oversight teams will use existing planned oversight activities for the compliance verification of the various Part IS implementation stages to the greatest extent possible.

The graph below illustrates the resulting oversight approach:



The organisations are expected to develop their Part IS system roughly following the green line.

Further details on the resulting oversight verification are available at the following link: https://www.easa.europa.eu/en/downloads/142683/en

Last updated:
26/09/2025

Link:
https://www.easa.europa.eu/pt/faq/142508

Continuous Improvement

Is there any specific maturity level that is required from the organisation following compliance?

Answer

While the rule does not specify a maturity level required for Part-IS compliance, it should be noted that, if and when compliance is achieved, organisations will determine which requirements of which models have already been met (mandatory) and can opt to reach a level that is beneficial to the organisation (voluntary).

In the longer term, achieving higher maturity levels may increase the confidence of oversight authorities, which can have an impact on the level of the oversight activities regarding such organisation.

Last updated:
22/08/2025

Link:
https://www.easa.europa.eu/pt/faq/142375

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?

Answer

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.

Last updated:
06/02/2024

Link:
https://www.easa.europa.eu/pt/faq/139304