CIVIL AVIATION DIRECTORATE
Airworthiness Inspectorate
Malta Transport Centre, Pantar Road, Lija LJA 2021 Malta Tel: +356 25555653 Fax: +356 21239278, civil.aviation@transport.gov.mt, www.transport.gov.mt

Transport Malta

Information and Advisory Notice No. 28

Issue No : 2 Dated : 13 October 2025

Part-IS (Information Security)

1. Introduction

The purpose of this IAN is to introduce the subject related to the new Regulation known as 'Part-IS', which is also applicable to **Part-CAMO** and **Part-145** organisations taking into consideration mainly the AMC and GM issued by EASA.

Information security impacts aviation safety and the scope of this regulation is to address the management of information security by organisations and service providers in a proportionate manner with the intent of safeguarding aviation safety and improve efficiency.

'information security' means the preservation of confidentiality, integrity, authenticity and availability of network and information systems.

'information security risk' means the risk to organisational civil aviation operations, assets, individuals, and other organisations due to the potential of an information security event. Information security risks are associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets.

2. Regulation

COMMISSION IMPLEMENTING REGULATION (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, … and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R0203

- Article 16
  This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall apply from **22 February 2026**.

- Annex II to Regulation EU No 2023/203 is **PART-IS.I.OR**

  IS.I.OR.100 Scope
  IS.I.OR.200 Information security management system (ISMS)
  IS.I.OR.205 Information security risk assessment
  IS.I.OR.210 Information security risk treatment
  IS.I.OR.215 Information security internal reporting scheme
  IS.I.OR.220 Information security incidents – detection, response, and recovery

IS.I.OR.225 Response to findings notified by the competent authority

IS.I.OR.230 Information security external reporting scheme
IS.I.OR.235 Contracting of information security management activities
IS.I.OR.240 Personnel requirements
IS.I.OR.245 Record-keeping
IS.I.OR.250 Information security management manual (ISMM)
IS.I.OR.255 Changes to the information security management system
IS.I.OR.260 Continuous improvement

- Annex VII to Regulation (EU) No 2023/203 contains the amendments to Part-145, Part-66 and Part-CAMO.

This annex introduces two new Headings:

- 145.A.200A Information security management system
- 145.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

- CAMO.A.200A Information security management system
- CAMO.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

Annex II to ED Decision 2023/009/R is the AMC and GM to Annex II

3. Main Elements of ISMS

The ISMS is modelled on SMS and this means that the pillars of SM can be utilised in ISMS.

In principle the organisation shall:

- **have a security policy and define the security scope and objectives**
- **appoint competent security personnel to manage IS**
- **have criteria for trustworthiness of responsible IS personnel**
- **have measures to detect, respond and recover from security incidents**
- **have Internal and external reporting schemes**
- **identify and define all key processes and procedures related to IS**
- **identify and manage security risks**
- **identify KPIs for information security**
- **measure and monitor KPIs for information security**
- **manage changes affecting IS**
- **implement compliance monitoring for effective implementation of the ISMS**
- **training and awareness of personnel**

Organisations shall refer to https://www.easa.europa.eu/community/system/files/2025-03/part-is-oversight-approach-guidelines_1.pdf for initial internal monitoring of the ISMS by compliance.

Security Risk assessment shall start from:

- The Identification of all relevant assets (i.e. **hardware, software, network and computing resources**) used to create, process, transmit, store or receive the operational inputs and outputs relevant to the **functions**, **services** and **capabilities** of the organisations.

- The Identification of the operating environments (e.g. office, public access area, access-controlled room, etc.) and locations for all relevant assets.

Since the organisations already have a management system, the current framework and structure for safety management may be used to integrate ISMS in the management system.

As in the case of Management Systems TM CAD will be also monitoring the effectiveness and maturity of the ISMS using the concept of the EASA MSAT.

It is required that the ISMS is **PRESENT** and **SUITABLE** at the time of the entry into force of the Part-IS regulation.

Outsourcing specific ISMS functions, such as information security monitoring or incident response to service providers, may help ensure that the organisation has access to experienced personnel and expertise. Similarly, organisations may want to be supported by a service provider in performing risk assessments.

EASA has devised an assessment matrix for the assessment of the ISM. The AI is representing this assessment tool in **AITP-A12 Appendix I**. This tool should be used and submitted to TM AD as part of the Part-IS implementation package.

4. Derogations

Organisations should follow the directions provided in AMC1 IS.I.OR.205(a) and AMC1 IS.I.OR.205(b) to perform a documented information security risk assessment to seek the approval by the TM CAD of a derogation under point IS.I.OR.200(e). The organization shall demonstrate to TM CAD that its activities, facilities and resources, as well as the services it operates, provides, receives and maintains, do not pose any information security risks with a potential impact on aviation safety neither to itself nor to other organisations.

5. Implementation

ISMS

For those Part-CAMO and Part-145 who fall under a common management system of an AOC, it is expected that these organisations utilise the implemented AOC Management System tools, policies and documentation to ensure consistency and avoid duplication.

It is recommended that for risk assessment criteria the organisations refer to **GM1 IS.I.OR.205(c) Information security risk assessment.** Interactions between security risks and aviation safety should also be taken into consideration.

ISMM

The ISMM may be submitted either as a separate document or integrated in the SM Manual (MSM) of the operator having al the items listed in **IS.I.OR.250 (a)**. When Manuals are integrated the listed Items in IS.I.OR.250 (a) shall be clearly indicated or cross-referred under the title headings or the index/LEPs.

It is important that during the implementation phase the Part-CAMO/Part-145 AMO indicates to the assigned Airworthiness Inspector the documents constituting the ISMM to ensure proper interface with the TM CAD Flight Operations Inspectorate for the review and final approval of the ISMM. Only one ISMM will be approved for an organisation having different approvals.

The contents of the ISMM shall be the following:

(1) a statement signed by the accountable manager confirming that the organisation will at all times work in accordance with this Annex and with the ISMM. If the accountable manager is not the chief executive officer (CEO) of the organisation, then the CEO shall countersign the statement;

(2) the title(s), name(s), duties, accountabilities, responsibilities and authorities of the person or persons defined in point IS.I.OR.240(b) and (c);

(3) the title, name, duties, accountabilities, responsibilities and authority of the common responsible person defined in point IS.I.OR.240(d), if applicable;

(4) the information security policy of the organisation as referred to in point IS.I.OR.200(a)(1);

(5) a general description of the number and categories of staff and of the system in place to plan the availability of staff as required by point IS.I.OR.240;

(6) the title(s), name(s), duties, accountabilities, responsibilities and authorities of the key persons responsible for the implementation of point IS.I.OR.200, including the person or persons responsible for the compliance monitoring function referred to in point IS.I.OR.200(a)(12);

(7) an organisation chart showing the associated chains of accountability and responsibility for the persons referred to in points (2) and (6);

(8) the description of the internal reporting scheme referred to in point IS.I.OR.215;

(9) the procedures that specify how the organisation ensures compliance with this Part, and in particular:
  (i) the documentation referred to in point IS.I.OR.200(c);
  (ii) the procedures that define how the organisation controls any contracted activities as referred to in point IS.I.OR.200(a)(9);
  (iii) the ISMM amendment procedure referred to in in point (c);

(10) the details of currently approved alternative means of compliance.

The ISMM shall contain the data retention policy of the organisation.

For independent CAMOs and Part-145 AMOs, the ISMM shall be submitted to the Airworthiness Inspectorate for review.

Personnel

The AM shall **appoint** a person or group of persons with the responsibility to ensure compliance with Part-IS.

The AM may also delegate his/her responsibility to a **Common Responsible Person** which would be normally referred to as (Chief) Information Security Officer, Cybersecurity Programme Director or Information Security Manager. This should be considered in case of multiple approvals, extensive contracting and multinational organisations. In such a case, coordination measures shall be established between the accountable manager of the organisation and the common responsible person to ensure adequate integration of the information security management within the organisation.

It is to be noted that the Part-IS regulation does not refer to nomination of a person or group of persons by the Accountable Manager for acceptance by the competent authority but appointment. However, the appointed personnel shall have the necessary competence and be trustworthy.

Part-IS AMC/GM includes provisions on how to evaluate competence and trustworthiness (due diligence) of personnel and this should be properly defined in the ISMM, implemented and recorded.

Personnel Competence

As stated in the AMC, to develop the **list of competencies**, an organisation may use, as initial guidance, an existing cybersecurity competence framework such as the NICE (National Initiative for Cybersecurity Education) based on the NIST Cybersecurity Framework (NIST CSF).

In Appendix II to AMC/GM, the main tasks of this Regulation are listed and mapped to the competencies derived from the NIST CSF. This mapping may be used to establish a baseline to identify the competence gaps. However, it should be noticed that existing cybersecurity/information security competence frameworks such as the NICE typically focus primarily on the protection of standard information technologies; therefore, the proposed list of competencies may need to be adapted to the technologies or integrated with processes used in the organisation.

Contracting of ISM activities

As per IS.OR.235 ISM activities may be contracted. In such case the organisation shall formalise this by means of a written executed agreement with the contractor.

GM3 IS.I.OR.236 provides examples of ISM activities which may be contracted.

When contracting out ISM activities the organisation shall pre-assess the contractor (competence, capability, manpower etc), manage the related security risks and include the contractor in the compliance monitoring plan of the organisation.

Transition

For those organisations with common management systems as part of an AOC holder the organisation shall follow OAN 04/25 issued by the Flight Operations Inspectorate of TM CAD for the timelines and submissions of the documentation and supporting evidence.

For those CAMO and Part-145 AMO that do not have a common management system under an

AOC or ATO, all submissions shall be made to the Airworthiness Inspectorate by the **30th October 2025.**

As part of the transition the organisation shall:

- Conduct a Management of Change exercise
- Submit an ISMM draft for review
- Submit the competence assessment of personnel performing activities covered by Part-IS
- Submit a manpower plan to cover to perform activities covered by Part-IS
- Submit an updated compliance audit plan
- Submit an internal audit report
- Submit any ISM activities contracts/agreements as applicable
- Submit a list of identified security hazards/risks and their risk level*
- PRESENT AND SUITABLE ISM Assessment (compiled AITP-A12 Appx 1 assessment tool)

*It is recognised that at the time of entry into force of the Regulation, the organisations may not be able to present a full security risk assessment (treatment) of their ISM from day one, however it is expected that the major security risks are identified and an initial assessment of risk assessed performed.

In case of any queries please do not hesitate to contact the lead airworthiness inspector for any clarifications.

References:
https://www.easa.europa.eu/community/topics/part-implementation-task-force-deliverables