Ensuring Compliance with EASA Information Security Management System (ISMS) Requirements DR EU 2022_1645

Sofema Online (SOL) www.sofemaonline.com considers the various requirements to be met for an organisation to demonstrate compliance with EASA Part-IS.D.OR (Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022) amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014.

Introduction

Potential Waiver - IS.D.OR.205 through IS.D.OR.260

If it (The organisation) demonstrates to the satisfaction of that authority 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.

The approval shall be based on a documented information security risk assessment carried out by the organisation or a third party in accordance with point IS.D.OR.205 and reviewed and approved by its competent authority.

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.

Contents

- IS.D.OR.100 – Scope
  - Establishes the requirements to be met by the organisations referred to in Article 2 of this Regulation. (Aerodrome, Design & Production Organisations – excluding ELA)

IS.D.OR.200 - Information security management system

- The processes, procedures, roles and responsibilities established by the organisation in order to comply with point IS.D. OR.200(a) shall correspond to the nature and complexity of its activities, based on an assessment of the information security risks inherent to those activities, and may be integrated within other existing management systems already implemented by the organisation.

The organisation shall set up, implement and maintain an information security management system (ISMS) which ensures that the organisation:

- Policy on information security with regard to the potential impact of information security risks on aviation safety;
- Identifies and reviews information security risks IS.D.OR.205;
- Security risk treatment measures in accordance with point IS.D.OR.210;
- IS internal reporting scheme in accordance with point IS.D.OR.215;
- Defines and implement measures IS.D.OR.220, the measures required to detect information security events (Emergency Response) alleviation for IS.D.OR.205(e)
- Comply with CA IS Requirements & action, in accordance with point IS.D.OR.225.
- External Reporting IS.D.OR.230
- Contracting activities to comply with IS.D.OR.235;
- Personnel requirements laid down in point IS.D.OR.240;
- Records IS.D.OR.245;
- Monitors compliance of the organisation IS requirements – feedback to AM or HOD (head of Design)
- Ensure incident reporting confidentiality
- continuous improvement process IS.D.OR.260.
- Document I.A.W IS.D.OR.250, establish a process for amending that documentation. Changes to those processes, procedures, roles and responsibilities shall be managed in accordance with point IS.D.OR.255.

IS.D.OR.205 - Information security risk assessment

The organisation shall identify all of its elements, which could be exposed to information security risks. That shall include:

- The organisation's activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains;
- The equipment, systems, data and information that contribute to the functioning of the elements listed
- The organisation shall identify the interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks.
- With regard to the elements and interfaces referred to, the organisation shall identify the information security risks which may have a potential impact on aviation safety.

    - For each identified risk, the organisation shall:

- Assign a risk level according to a predefined classification established by the organisation;
- Associate each risk and its level with the corresponding element or interface identified
- The predefined classification shall take into account the potential of occurrence of the threat scenario and the severity of its safety consequences.
- Based on that classification, and taking into account whether the organisation has a structured and repeatable risk management process for operations, the organisation shall be able to establish whether the risk is acceptable or needs to be treated in accordance with point IS.D.OR.210.

Note - assignment of the risk level shall take into account all relevant information

Review and update the risk assessment when:

- There is a change in the elements subject to information security risks;
- There is a change in the Organisational Interfaces
- There is a change in the information or knowledge used for the identification, analysis and classification of risks;
- There are lessons learnt from the analysis of information security incidents.

IS.D.OR.210 - Information Security Risk Treatment

Those measures shall enable the organisation to:

- Control the circumstances that contribute to the effective occurrence of the threat scenario;
- Reduce the consequences on aviation safety associated with the materialisation of the threat scenario;
- Avoid the risks. (Measures shall not introduce any new potential unacceptable risks to aviation safety.

Communication of Risk Assessment & Outcome Measures (IS.D.OR.240) – AM and interface organisations

- shall also inform interface organisations of any risk shared between both organisations.

IS.D.OR.215 - Information security internal reporting scheme

Establish an internal reporting scheme (IS.D.OR.230)

Scheme and process ref IS.D.OR.220 to:

- Identify which of the events are considered information security incidents or vulnerabilities with a potential impact on aviation safety;
- Identify the causes of, and contributing factors to, the information security incidents and vulnerabilities identified
- Address them as part of the information security risk management process in accordance with points IS.D.OR.205 and IS.D.OR.220;

- Ensure an evaluation of all known, relevant information relating to the information security incidents and vulnerabilities identified
- Ensure the implementation of a method to distribute internally the information as necessary.
- Contracted Organisations required to report IS Events I.A.W contracted procedure
- Cooperate on investigations with any other organisation that has a significant contribution to the information security of its own activities.
- May Integrate that reporting scheme with other reporting schemes it has already implemented.

IS.D.OR.220 - Information security incidents – detection, response, and recovery

Based on the outcome of the risk assessment - shall implement measures to detect incidents and vulnerabilities that indicate the potential materialisation of unacceptable risks and which may have a potential impact on aviation safety.

Those detection measures shall enable the organisation to:

- Identify deviations from predetermined functional performance baselines;
- Trigger warnings to activate proper response measures, in case of any deviation.
- Implement measures to respond to any event conditions that may develop or have developed into an information security incident.
- Those response measures shall enable the organisation to:
  - Initiate the reaction to the warnings by activating predefined resources and course of actions;
  - Contain the spread of an attack and avoid the full materialisation of a threat scenario;
  - Control the failure mode of the affected elements defined in point IS.D.OR.205(a).

- The organisation shall implement measures aimed at recovering from information security incidents, including emergency measures, i
- Those recovery measures shall enable the organisation to:
    - Remove the condition that caused the incident, or constrain it to a tolerable level;
    - Reach a safe state of the affected elements defined in point IS.D.OR.205(a) within a recovery time previously defined by the organisation.

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

After receipt of the notification of findings submitted by the competent authority, the organisation shall:

- Identify the root cause or causes of, and contributing factors to, the non-compliance;
- Define a corrective action plan;
- Demonstrate the correction of the non-compliance to the satisfaction of the competent authority.
- The actions required shall be carried out within the period agreed with the competent authority.

IS.D.OR.230 - Information security external reporting scheme

- IS reporting system Compliant with (EU) No 376/2014.
- Shall report to CA information security incident or vulnerability, which may represent a significant risk to aviation safety
    - Where such an incident or vulnerability affects an aircraft or associated system or component, the organisation shall also report it to the design approval holder;

- Notification submitted to the CA & DAH or to the organisation responsible for the design of the system or constituent, as soon as the condition has been known to the organisation; (ASAP – not exceeding 72 hours)

- Follow-up report submitted to the CA and DAH providing details of the actions the organisation has taken or intends to take to recover from the incident and the actions it intends mitigate. (as soon as practicable)

IS.D.OR.235 - Contracting of information security management activities

- Contracted activities comply with the requirements of this Regulation and the contracted organisation works under its oversight.

- The organisation shall ensure that the risks associated with the contracted activities are appropriately managed.
- Competent authority can have access upon request to the contracted organisation to determine continued compliance with the applicable requirements laid down in this Regulation.

IS.D.OR.240 - Personnel requirements

- AM or HOD - corporate authority to ensure that all activities required by this Regulation can be financed and carried out.
    - Ensure that all necessary resources are available to comply with the requirements of this Regulation;
    - Establish and promote the information security policy
    - Demonstrate a basic understanding of this Regulation.

- Shall Appoint a person or group of persons to ensure that the organisation is in compliance with the requirements of this Regulation, and shall define the extent of their authority.
    - Shall report directly to the AM or HOD
    - Procedures identify Deputy (Lengthy Absence)
- Shall appoint a person or persons to monitor compliance
- May integrate and share – Common responsible person
    - Common responsible person to ensure adequate integration of the information security management within the organisation.

- Sufficient Personnel for activities covered by this Annex.
- Personnel shall be competent to perform their tasks.
- Process in place to ensure that personnel acknowledge the responsibilities associated with the assigned roles and tasks.
- The organisation shall ensure that the identity and trustworthiness of the personnel who have access to information systems and data subject to the requirements of this Regulation are appropriately established.

IS.D.OR.245 - Record-keeping

The format of the records shall be specified in the organisation’s procedures.

Shall keep records of its information security management activities - archived and traceable:

- Any approval received and any associated information security risk assessment in accordance with point IS.D. OR.200(e);
- Contracts for activities referred to in point IS.D.OR.200(a)(9);

- Records of the key processes referred to in point IS.D.OR.200(d);
- Records of the risks identified in the risk assessment referred to in point IS.D.OR.205 along with the associated risk treatment measures referred to in point IS.D.OR.210;
- Records of information security incidents and vulnerabilities reported in accordance with the reporting schemes referred to in points IS.D.OR.215 and IS.D.OR.230;
- Records of those information security events which may need to be reassessed to reveal undetected information security incidents or vulnerabilities.

Records retained at least until 5 years after the approval has lost its validity.

Contract records retained at least until 5 years after the contract has been amended or terminated.

Qualifications & Experience

The organisation shall keep records of qualification and experience of its own staff involved in information security management activities Records at least 3 years after the person has left the organisation.

- Access to own records & copy when leaving

The organisation shall ensure that the records are stored using means to ensure integrity, authenticity and authorised access.

IS.D.OR.250 - Information security management manual (ISMM)

The initial issue of the ISMM shall be approved and a copy shall be retained by the competent authority. The ISMM shall be amended as necessary to remain an up-to-date description of the ISMS of the organisation. A copy of any amendments to the ISMM shall be provided to the competent authority.

The organisation may integrate the ISMM with other management expositions or manuals it holds, provided there is a clear cross reference that indicates which portions of the management exposition or manual correspond to the different requirements contained in this Annex.

- Available to CA - (ISMM) and, where applicable, any referenced associated manuals and procedures, containing:
    - Statement signed by the accountable manager or, HOD
    - Details of all relevant persons

- IS Policy
- Number and categories of staff and of the system in place to plan the availability of staff as required by point IS.D.OR.240;
- Organogram chains of accountability and responsibility for the persons referenced
- Description of the internal reporting scheme referred to in point IS.D.OR.215;
- Procedures to demonstrate compliance with ISD requirements
- How the organisation controls contracted activities.
- Amendment procedures
- Approved alternative means of compliance.

IS.D.OR.255 - Changes to the information security management system

- Changes Managed & Notified to CA
- Changes to the ISMS not covered by the procedure shall apply for and obtain an approval issued by the competent authority.
- Application shall be submitted before any such change takes place, in order to enable the competent authority to determine continued compliance with this Regulation and to amend, if necessary, the organisation certificate and related terms of approval attached to it;
    - Shall make available to the competent authority any information it requests to evaluate the change;
    - Change shall be implemented only upon receipt of a formal approval by the competent authority;
    - Shall operate under the conditions prescribed by the competent authority during the implementation of such changes.

IS.D.OR.260 - Continuous improvement

- Shall assess, using adequate performance indicators, the effectiveness and maturity of the ISMS.
- Assessment shall be carried out on a calendar basis predefined by the organisation or following an information security incident.
    - Any deficiencies found following the assessment - the organisation shall take the necessary improvement measures to ensure that the ISMS continues to comply with the applicable requirements and maintains the information security risks at an acceptable level.
    - In addition, the organisation shall reassess those elements of the ISMS affected by the adopted measures.