Back to Basics – What are the Part IS Regulatory Obligations?

IS.D.OR.200 Information security management system (ISMS) - *Regulation (EU) 2022/1645*

(a) In order to achieve the objectives set out in Article 1, the organisation shall set up, implement and maintain an information security management system (ISMS) which ensures that the organisation:

(1) establishes a policy on information security setting out the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;

(2) identifies and reviews information security risks in accordance with point IS.D.OR.205;

IS.D.OR.205 Information security risk assessment
Regulation (EU) 2022/1645
(a) The organisation shall identify all of its elements, which could be exposed to information security risks. That shall include:
(1) the organisation's activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains;
(2) the equipment, systems, data and information that contribute to the functioning of the elements listed in point (1).
(b) 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 in points (a) and (b), the organisation shall identify the information security risks which may have a potential impact on aviation safety. For each identified risk, the organisation shall:
(1) assign a risk level according to a predefined classification established by the organisation;
(2) associate each risk and its level with the corresponding element or interface identified in accordance with points (a) and (b).

The predefined classification referred to in point (1) 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.
In order to facilitate the mutual comparability of risks assessments, the assignment of the risk level pursuant to point (1) shall take into account relevant information acquired in coordination with the organisations referred to in point (b).

(d) The organisation shall review and update the risk assessment carried out in accordance with points (a), (b) and (c) in any of the following situations:
(1) there is a change in the elements subject to information security risks;
(2) there is a change in the interfaces between the organisation and other organisations, or in the risks communicated by the other organisations;
(3) there is a change in the information or knowledge used for the identification, analysis and classification of risks;
(4) there are lessons learnt from the analysis of information security incidents.

(3) defines and implements information security risk treatment measures in accordance with point IS.D.OR.210;

IS.D.OR.210 Information security risk treatment
Regulation (EU) 2022/1645
(a) The organisation shall develop measures to address unacceptable risks identified in accordance with point IS.D.OR.205, implement them in a timely manner and check their continued effectiveness. Those measures shall enable the organisation to:
(1) control the circumstances that contribute to the effective occurrence of the threat scenario;
(2) reduce the consequences on aviation safety associated with the materialisation of the threat scenario;
(3) avoid the risks.
Those measures shall not introduce any new potential unacceptable risks to aviation safety.
The person referred to in point IS.D.OR.240(a) and (b) and other affected personnel of the organisation shall be informed of the outcome of the risk assessment carried out in accordance with point IS.D.OR.205, the corresponding threat scenarios and the measures to be implemented.
The organisation shall also inform organisations with which it has an interface in accordance with point IS.D.OR.205(b) of any risk shared between both organisations.

(4) implements an information security internal reporting scheme in accordance with point IS.D.OR.215;

IS.D.OR.215 Information security internal reporting scheme
Regulation (EU) 2022/1645
(a) The organisation shall establish an internal reporting scheme to enable the collection and evaluation of information security events, including those to be reported pursuant to point IS.D.OR.230.
(b) That scheme and the process referred to in point IS.D.OR.220 shall enable the organisation to:

(1) identify which of the events reported pursuant to point (a) are considered information security incidents or vulnerabilities with a potential impact on aviation safety;
(2) identify the causes of, and contributing factors to, the information security incidents and vulnerabilities identified in accordance with point (1), and address them as part of the information security risk management process in accordance with points IS.D.OR.205 and IS.D.OR.220;
(3) ensure an evaluation of all known, relevant information relating to the information security incidents and vulnerabilities identified in accordance with point (1;)
(4) ensure the implementation of a method to distribute internally the information as necessary.
(c) Any contracted organisation which may expose the organisation to information security risks with a potential impact on aviation safety shall be required to report information security events to the organisation. Those reports shall be submitted using the procedures established in the specific contractual arrangements and shall be evaluated in accordance with point (b).
(d) The organisation shall cooperate on investigations with any other organisation that has a significant contribution to the information security of its own activities.
(e) The organisation may integrate that reporting scheme with other reporting schemes it has already implemented.

(5) defines and implements, in accordance with point IS.D.OR.220, the measures required to detect information security events, identifies those events which are considered incidents with a potential impact on aviation safety except as permitted by point IS.D.OR.205(e), and responds to, and recovers from, those information security incidents;

IS.D.OR.220 Information security incidents — detection, response and recovery
Regulation (EU) 2022/1645
(a) Based on the outcome of the risk assessment carried out in accordance with point IS.D.OR.205 and the outcome of the risk treatment performed in accordance with point IS.D.OR.210, the organisation 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:
(1) identify deviations from predetermined functional performance baselines;
(2) trigger warnings to activate proper response measures, in case of any deviation.
(b) The organisation shall implement measures to respond to any event conditions identified in accordance with point (a) that may develop or have developed into an information security incident. Those response measures shall enable the organisation to:

(1) initiate the reaction to the warnings referred to in point (a)(2) by activating predefined resources and course of actions;
(2) contain the spread of an attack and avoid the full materialisation of a threat scenario;
(3) control the failure mode of the affected elements defined in point IS.D.OR.205(a).
(c) The organisation shall implement measures aimed at recovering from information security incidents, including emergency measures, if needed. Those recovery measures shall enable the organisation to:
(1) remove the condition that caused the incident, or constrain it to a tolerable level;
(2) 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.

(6) implements the measures that have been notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety;

(7) takes appropriate action, in accordance with point IS.D.OR.225, to address findings notified by the competent authority;

(8) implements an external reporting scheme in accordance with point IS.D.OR.230 in order to enable the competent authority to take appropriate actions;

(9) complies with the requirements contained in point IS.D.OR.235 when contracting any part of the activities referred to in point IS.D.OR.200 to other organisations;

(10) complies with the personnel requirements laid down in point IS.D.OR.240;

(11) complies with the record-keeping requirements laid down in point IS.D.OR.245;

(12) monitors compliance of the organisation with the requirements of this Regulation and provides feedback on findings to the accountable manager or, in the case of design organisations, to the head of the design organisation, in order to ensure effective implementation of corrective actions; ***Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645)*** *Delegated Regulation (EU) 2022/1645 ANNEX — INFORMATION SECURITY — ORGANISATION REQUIREMENTS [PART-IS.D.OR]*

(13) protects, without prejudice to applicable incident reporting requirements, the confidentiality of any information that the organisation may have received from other organisations, according to its level of sensitivity.

(b) In order to continuously meet the requirements referred to in Article 1, the organisation shall implement a continuous improvement process in accordance with point IS.D.OR.260.

(c) The organisation shall document, in accordance with point IS.D.OR.250, all key processes, procedures, roles and responsibilities required to comply with point IS.D.OR.200 (a) and 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.

(d) 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.

(e) Without prejudice to the obligation to comply with the reporting requirements contained in Regulation (EU) No 376/2014(1) and the requirements of point IS.D.OR.200(a)(13), the organisation may be granted approval by the competent authority not to implement the requirements referred to in points (a) to (d)) and the related requirements contained in points IS.D.OR.205 through IS.D.OR.260, if it 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.