Guidelines

ISO/IEC 27001 vs PART-IS

Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS[*]

Part-IS TF G-01

July 2024

"This document has been developed by the Part-IS Implementation Task Force, a collaborative effort of EASA States civil aviation authorities. The Task Force has worked with great care to produce a comprehensive set of guidelines aimed at ensuring a harmonised implementation of Part-IS across Member States. This initiative is part of the ongoing commitment to maintain high standards of aviation safety throughout the European Union."

[*] A set of rules contained in Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 and in Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down requirements for the management of information security risks with a potential impact on aviation safety for aviation organisations and authorities across the entire aviation domain.

Guidelines

ISO/IEC 27001 vs PART-IS

Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS

Document ref.	Status	Date
Part-IS TF G-01	Issued	15/07/2024
Contact name and address for enquiries:	cybersec@easa.europa.eu European Aviation Safety Agency Cybersecurity and Emerging Risks Section Postfach 10 12 53 50452 Köln Germany	
Information on EASA is available at:	www.easa.europa.eu	

This document is published on the basis of Article 1(3)(f) of Regulation (EU) 2018/1139 which states that the objectives of that Regulation shall be achieved by, inter alia: 'the uniform implementation of all necessary acts by the national competent authorities and the Agency, within their respective areas of responsibility;'. Of relevance is one of the objectives enshrined in Article 1(2), namely to 'promote cost-efficiency, by, inter alia, avoiding duplication, and promoting effectiveness in regulatory, certification and oversight processes as well as an efficient use of related resources at Union and national level;'

This document is also published in conjunction with Art. 5(3) of Regulation (EU) No 628/2013: "The Agency shall rovide competent authorities of Member States with relevant information to support the uniform implementation of the applicable requirements."

Authorisation :

	Name	Signature	Date
Prepared	N/A	N/A	-
Reviewed 1	N/A	Adopted by Part-IS Task Force	15/07/2024

Table of Contents

1 Executive summary

The term "Part-IS" represents the information security management system (ISMS)requirements laid down in the Regulations of the European Union (EU) 2022/1645 (Delegated Regulation) and (EU) 2023/203 (Implementing Regulation). These regulations introduce provisions for Information Security Management System (ISMS in relation to). It applies to aviation organisations and to the authorities responsible for their certification and oversight. The main objective of this ISMS is to properly control information secuity risks that may have an impact on aviation safety. Both regulations are available free of charge from the "EUROLEX" website in all languages of the European Union.

The applicability of Part-IS to organisations and authorities is determined in Article 2 of the regulations.

There are cases where organisations and authorities subject to Part-IS have already implemented an ISMS in response to business needs, or general strengthening of their organisation's security to better protect their organisation. The most widely adopted standard for ISMS is ISO/IEC27001:2022, later referred to as IISO/IEC 27001.

As Part-IS shares similar provisions as ISO/IEC 27001, the EASA Part-IS implementation Task Force have developed this guidance document to support organisations with existing ISMS conforming to ISO/IEC 27001:2022 to integrate Part-IS into their existing ISMS.

2 How to read this document

To facilitate easy referencing, this document is presented using the same order of requirements found in Part-IS.

- For each requirement, the original Part-IS text is rewritten under the heading “Requirement”, in blue.
- Next, the counterpart provision of ISO/IEC 27001:2022 (equivalent or partially equivalent) is stated as “ISO/IEC 27001 mapping” in yellow. (Mappings in brackets are no direct match)
- This is followed by an explanation of “Part-IS particularity” in red, versus ISO/IEC 27001 for that requirement.

Finally, guidance for Part-IS implementation in green, demonstrates how to integrate this particularity into an existing ISO/IEC 27001 based ISMS to achieve Part-IS compliance.

As certificates for ISMS based on ISO/IEC 27001:2013 are not valid after October 2025 and Part-IS becomes applicable in October 2025 or February 2026 (latest), this guidance document refers only to ISO/IEC 27001:2022.

As the requirements of IS.I.OR (Reg. (EU) 2023/203) and IS.D.OR (Reg. (EU) 2022/1645) are identical, this guidance document refers to “IS.OR” implying both covered.

2.1 Example on IS.OR.235 (a) Contracting of ISM activities

Requirement

The unmodified requirement of Part-IS

a) `The organisation shall ensure that when contracting any part of the activities referred to in point IS.I.OR.200 to other organisations, the 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.

b) ISO/IEC 27001 mapping

The ISO/IEC 27001 counterpart to the requirement

A5.19 Information security in supplier relationships

A5.21 Managing information security in the information and communication technology (ICT) supply chain

A5.22 Monitoring, review and change management of supplier services

Part-IS particularity

The reason for a specific Part-IS guidance

ISO/IEC 27001 controls A5.19, A5.21 and A5.29 may cover this requirement. The difference in the requirements of IS.OR.235 is, that it is limited to those activities directly related to the ISMS (e. g. internal audits, consultancy for risk assessments, ….).

In addition, all “domain specific” implementation rules (e.g. ORO.AOC.110, ORA.GEN.205, CAMO.A.205, 145.A.205, 21.A.139 (d) (1), 21.A.239 (d) (3), ATM/ANS.OR.B.020, ATCO.OR.C.005, ADR.OR.D.010,) of Reg. (EU) 2018/1139 require procedures to deal with contracted activities in a wider scope, where information security should be integrated.

The add-on guidance

Guidance for Part-IS implementation

The difference in the requirements of IS.OR.235 is, that it is limited to those activities directly related to the ISMS (e. g. internal audits, consultancy for risk assessments, ….). The controls in ISO/IEC 27001 do not exclude those kinds of services, but sometimes it will not be in the focus of the organisation.

Therefore, there is no need to establish an independent system for those contractors mentioned IS.OR.235 (a). The list of suppliers should be reviewed to ensure, that the suppliers providing the services mentioned in IS.OR.235 are covered.

3 Other background information

3.1 Easy Access Rules

EASA also publishes so called "Easy Access Rules", where the Regulation, the "Acceptable Means of Compliance" (AMC) and the "Guidance Material" (GM) are combined into one single document. These "Easy Access Rules" are free of charge and available in PDF, XML and On-line format on the EASA website.

Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645) - Revision from June 2024 — Available in pdf, online & XML format | EASA (europa.eu)

3.2 Acceptable Means of Compliance and Guidance Material

According to the European rulemaking process for aviation, additional information material to assist in the implementation of the regulations was developed. This material covers two groups of information:

Acceptable Means of Compliance are non-binding. The AMC serves as a means by which the requirements contained in the Regulations can be met. However, applicants may decide to show compliance with the requirements using other means. Both CAAs and organisations may propose 'Alternative Means of Compliance' These 'Alternative Means of Compliance' proposals must be accompanied by evidence of their ability to meet the intent of the IR. Use of an existing AMC gives the user the benefit of compliance with the IR.

Guidance Material is non-binding explanatory and interpretation material on how to achieve the requirements contained in the Regulations and the AMCs. It contains information, including examples, to assist the user in the interpretation and application of the Regulations and the AMCs.

4 Information security management system (ISMS)

4.1 IS.OR.200 (a) Information security mangement system (ISMS)

Requirement

(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.I.OR.205;

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

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

(5) defines and implements, in accordance with point IS.I.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.I.OR.205(e), and responds to, and recovers from, those information security incidents;

(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.I.OR.225, to address findings notified by the competent authority;

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

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

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

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

(12)monitors compliance of the organisation with the requirements of this Regulation and provides feedback on findings to the accountable manager to ensure effective implementation of corrective actions;

(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.

ISO/IEC 27001 mapping

4. Context of the organisation

6.1.1 Actions to address risks and opportunities - General

Part-IS particularity

An information security management system designed in the context of an ISO/IEC 27001 ISMS, which is currently not connected to the management systems required by the implementing rules of Reg. (EU) 2018/1139, and in the context of Part-IS, may differ if they do not address the same goals. Part-IS focuses on information security requirements meeting the applicable aviation safety objectives, which have an influence on elements of the information security management system.

Also the "interested parties" and the "internal and external issues" as laid down in chapter 4 of ISO/IEC 27001 may be adapted to address the requirements of Part-IS for the organisation.

Guidance for Part-IS implementation

Please note that the OR.200 requirement points to many other Part-IS requirements that the expected ISMS has to comply with. Namely: 205, 210, 215, 220, 225, 230, 235, 240,245, 255, and 260. We will dive into further detail in the specific chapters of the particular requirement.

Regarding the other remaining requirements, not pointing out to other PART-IS requirements, and comparing them with ISO/IEC 27001, there are four requirements left, namely IS.OR.200.a.1, IS.OR.200.a.6, IS.OR.200.a.12, and IS.OR.200.a.13. These requirements are described in this chapter:

4.2 IS.OR.200 (a)(1) Information security management system (ISMS)

Requirement

(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;

ISO/IEC 27001 mapping

5.2 Policy

A.5.1 Policies for information securities

Part-IS particularity

An information security management system designed in the context of an ISO/IEC 27001 ISMS, which is currently not connected to the management systems required by the implementing rules of Reg. (EU) 2018/1139, may differ as they do often not address the same goals. Part-IS focuses on information security requirements influencing the applicable aviation safety objectives, which vice versa have an influence on the elements of the information security management system.

In addition, all domain-specific implementing regulations (namely ORO.GEN.200 (a) (2), ORA.GEN.200 (a) (2), CAMO.A. 200 (a) (2), 145.A.200 (a) (2), 21.A.139 (c) (1), 21.A.239 (c) (1), ATM/ANS.OR.B.005 (a) (2), ATCO.OC.C.001 (b), ADR.OR.D.005 (b) (2),) of Reg. (EU) 2018/1139) require a "safety policy", where information security may be integrated.

Guidance for Part-IS implementation

The policy on information security established in an ISO/IEC 27001 context **shall be updated with regard to the potential impact of the risks on aviation safety**. At least the elements of **AMC1 IS.I.OR.200 (a)(1)** shall be mentioned in the policy. The following elements in bold probably need to be added to an existing ISMS policy. The elements in bold and italics are additional guidance that might also be considered.

(a) committing to comply with applicable legislation, consider relevant standards and best practices, ***including safety and cybersecurity related standards and guidance published or prescribed by ICAO, EASA, or the relevant civil aviation authority***;

(b) setting objectives and performance measures for managing information security, ***updated to ensure meeting*** the applicable aviation safety objectives;

(c) defining general principles, activities, processes for the organisation to appropriately secure information and communication technology systems and data, ***in relation to the information security / safety risk assessment required by IS.OR.205***;

(d) committing to apply ISMS requirements into the processes of the organisation;

(e) committing to continually improve **towards higher levels of information security process maturity** as per IS.I.OR.260;

(f) committing to satisfy applicable requirements regarding information security ***(including requirements stemming from civil aviation authorities)*** and its proactive and systematic management and to the provision of appropriate resources for its implementation and operation;

(g) assigning information security as one of the essential responsibilities **for all managers**;

(h) committing to promote the information security policy through training or awareness sessions within the organisation to all personnel on a regular basis or upon modifications;

(i) **encouraging the implementation of a 'just-culture'** and the reporting of vulnerabilities, suspicious/anomalous events and/or information security incidents;

(j) committing to communicate the information security policy to all relevant parties, as appropriate.

4.3 IS.OR.200 (a)(6) Information security management system (ISMS)

Requirement

(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.

ISO/IEC 27001 mapping

(10.1 Corrective actions)

(A5.5 Contact with authorities)

(A5.26 Response to information security incidents)

(A8.8 Management of technical vulnerabilities)

Part-IS particularity

This requirement does not have a direct representation in ISO/IEC 27001.

However, most domain-specific implementing regulations (namely ORO.GEN.155, ORA.GEN.155, CAMO.A.155, 145.A.155, ATM/ANS.OR.A.060, ATCO.OR.B.035, ADR.OR.C.025) of Reg. (EU) 2018/1139 require a similar function, which may be used.

Guidance for Part-IS implementation

The policies and procedures, defined as means of compliance to the requirements listed above should be extended to information security measures mandated by the competent authority.

Note: Organisations also falling under the "NIS-regime", transposed into their national regulation, need to consider measures mandated by the competent authority for NIS in this function.

4.4 IS.OR.200 (a)(12) Information security management system (ISMS)

Requirement

(12) monitors compliance of the organisation with the requirements of this Regulation and provides feedback on findings to the accountable manager to ensure effective implementation of corrective actions.

ISO/IEC 27001 mapping

9.2. Internal audit

9.3 Management review

10.2 Non-conformity and corrective action

A5.36 Compliance with policies, rules and standards for information security

Part-IS particularity

This requirement is strongly related to the internal audit system and the independent checking function of ISO/IEC 27001. The required feedback system to the accountable manager fits into the requirement of 9.3.

In addition, all domain-specific implementing regulations (namely ORO.GEN. (a) (6), ORA.GEN.200 (a) (6), CAMO.A. 200 (a) (6), 145.A.200 (a) (6), 21.A.139 (e), 21.A.239 (d) (2), ATM/ANS.OR.B.005 (c), ATCO.OR.C.001 (f), ADR.OR.D.005 (b) (11),) of Reg. (EU) 2018/1139 require a similar "compliance monitoring function", where information security should be integrated.

AMC1 IS.OR.200 (a)(12) directly refers to this integration.

Guidance for Part-IS implementation

The requirements of ISO/IEC 27001 and the implementing rules of Reg. (EU) 2018/1139 are compatible. Therefore, it will be easy to add Part-IS into the audit scope of the ISO/IEC 27001 internal audit system.

The role of the Accountable Manager as defined under IS.OR.240 (a) shall be addressed accordingly in the feedback loop if the role is not already addressed in the management review process. It is required that the accountable manager is personally briefed on the key findings so that appropriate decisions can be made.

Refer also to GM1 IS.I.OR.200 (a)(12).

Nevertheless, **AMC2 CAMO.A.200 (a)(6)** as an example of the understanding for how the internal audit system should be used for audit compliance, is a good reference for all domains (*references to Part-CAMO were purged for better readability for other domains*):

COMPLIANCE MONITORING — INDEPENDENT AUDIT

(a) An essential element of compliance monitoring is the independent auditing.

(b) The independent auditing is an objective process. It involves routine sample checks of all aspects of the organisation's ability to carry out continuing airworthiness management to the standards required by this Regulation. It should include some product/service sampling as this is the end result of the process.

(c) The independent audit should provide an objective overview of the complete set of business related activities.

(d) The organisation should establish an audit plan to show when and how often the activities will be audited.

(e) The audit plan should ensure that all aspects of compliance are verified each year, including any sub-contracted activities. The audit may be carried out as a complete single exercise or subdivided over the annual period. The independent audit should not require each procedure to be verified for each product or service if it can be demonstrated that the particular procedure is common to more than one product line and the procedure has been verified each year with no findings. Where findings have been identified, the particular procedure should be verified against other product lines until the findings have been closed, after which the independent audit procedure may revert to a yearly interval for the particular procedure.

(f) Provided that there are no safety-related findings, the audit planning cycle specified in this AMC may be increased by up to 100 %, subject to a risk assessment and/or mitigation actions, and agreement by the competent authority.

(g) Where the organisation has more than one approved site, the audit plan should ensure that each site is audited every year or at a periodicity determined through a risk assessment agreed by the competent authority and in any case not exceeding the applicable audit planning cycle.

(h) A report should be issued each time an audit is carried out describing what was checked and the resulting non-compliance findings against applicable requirements and procedures.

Note: *ISO19011:2018 provides guidance for the establishment of an internal audit system. Specifically, chapter A.7 "Auditing compliance within a management system" gives useful guidance to integrate a compliance monitoring function into an internal audit system.*

4.5 IS.I.OR.200 (a)(13) Information security management system (ISMS)

Requirement

(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.

ISO/IEC 27001 mapping

7.5.3. Control of documented information (Note)

A5.12 Classification of information

A5.34 Privacy and protection of personal identifiable information (PII)

A8.12 Data leakage prevention

Part-IS particularity

This requirement is limited to “information from other organisations” and to confidentiality. ISO/IEC 27001 does not differ between “internal” or “external” information (as laid down e.g. in ISO 9001:2015 chapter 8.5.3). The only reference is made in the note in chapter 7.5.3.

Part-IS stresses protection of external information received due to the sensitivity it may have regarding incidents and vulnerabilities disclosure. Insufficient confidentiality protection may result in exploitation of vulnerabilities affecting safety that the original provider of information may not have perceived.

Guidance for Part-IS implementation

The protection of information, specifically regarding confidentiality (as in ISO 27002:2022), is related to a huge set of controls. Table A.1 (Matrix of controls and attribute values) in ISO 27002:2022 gives a comprehensive overview of these controls.

See also the definition in ISO 27002:2022:

3.1.7 confidential information

information that is not intended to be made available or disclosed to unauthorized individuals, entities or processes.

The organization having implemented these controls should take special care that they apply to information received from external information that may result in information security threats if known by unauthorized actors. When this kind of information is further shared with other organizations or authorities, appropriate confidentiality procedures must be put in place and followed (TLP marking for instance).

4.6 IS.OR.200 (b) Information security management system (ISMS)

Requirement

(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.I.OR.260.

ISO/IEC 27001 mapping

10.1 Continual improvement

Part-IS particularity

Part-IS and ISO/IEC 27001 are very similar regarding this requirement. See IS.OR.260 (a) and (b) for subtle differences.

Guidance for Part-IS implementation

The guidance is given under IS.OR.260.

4.7 IS.OR.200 (c) Information security management system (ISMS)

Requirement

(c) The organisation shall document, in accordance with point IS.I.OR.250, all key processes, procedures, roles and responsibilities required to comply with point IS.I.OR.200 (a) and shall establish a process for amending that documentation. Changes to those processes, procedures, roles and responsibilities shall be managed in accordance with point IS.I.OR.255.

ISO/IEC 27001 mapping

6.3 Planning of changes

7.5.3 Control of documented information

Part-IS particularity

Control of documented information is one of the key processes in each ISO management system standard, following the ISO “high level structure” (ISO/IEC Directives part 1 Annex SL), such as ISO/IEC 27001 :2022.

For Changes see IS.OR.255.

In addition, most “domain specific” implementation rules (namely ORO.GEN. (a) (5), ORA.GEN.200 (a) (5), CAMO.A. 200 (a) (5), 145.A.200 (a) (5), 21.A.139 (a), ATM/ANS.OR.B.005 (b), ATCO.OR.01 (e), ADR.OR.D.005 (c),) of Reg. (EU) 2018/1139 require a similar need to document, where information security should be integrated.

Guidance for Part-IS implementation

Additional guidance is given under IS.OR.250 and IS.OR.255.

4.8 IS.OR.200 (d) Information security management system (ISMS)

Requirement

(d) The processes, procedures, roles and responsibilities established by the organisation in order to comply with point IS.I.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.

ISO/IEC 27001 mapping

4.3 Determining the scope of the information security management system.

Part-IS particularity

The scope statement and the “statement of applicability” (SOA) are the best references to apply the “nature and complexity”.

In addition, all domain-specific implementing regulations (namely, ORO.GEN. (b) ORA.GEN.200 (b), CAMO.A. 200 (b), 145.A.200 (b), 21.A.139 (b) 1, 21.A.239 (b) (1), ATM/ANS.€B.005 (e), ATCO.OR.C.001 (g), ADR.OR.D.005 (d),) of Reg. (EU) 2018/1139 require a similar need for documentation, where information security may also be integrated.

Guidance for Part-IS implementation

When determining the scope, it should be noted that Part-IS is delimited to the subject matter as defined in Article 1 of the Regulation(s).

Article 1 – Subject matter

This Regulation sets out the requirements to be met by the organisations and competent authorities in order:

(a) to identify and manage information security risks ***with potential impact on aviation safety*** *which could affect information and communication technology systems and data used for civil aviation purposes,*

(b) to detect information security events and identify those which are considered information security incidents ***with potential impact on aviation safety,***

(c) to respond to, and recover from, those information security incidents.

Considering this, an ISMS under ISO/IEC 27001 may have a wider scope than required by Part-IS. It could be the case, that some organisational unit, processes or locations of an organisation might be covered by the ISMS under ISO/IEC 27001, but not applicable to Part-IS. To reduce complexity, it is advised to voluntarily implement Part-IS also for those processes.

The opposite may happen too: the scope under ISO/IEC 27001 may be narrower than the one Part-IS would require (e. g. the ISO/IEC 27001 scope covers only the IT-department).

In both situations scope definitions must be compared and adjusted when necessary.

Note: see also guidance to IS.OR.205 (a)

The Scope-statement in the ISO/IEC 27001 context is the right place, where this clarification is ma€

4.9 IS.OR.200 (e) Information security management system (ISMS)

Requirement

(e) Without prejudice to the obligation to comply with the reporting requirements laid down in Regulation (EU) No 376/2014 (1) and the requirements laid down in point IS.I.OR.200(a)(13), the organisation may be approved by the competent authority not to implement the requirements referred to in points (a) to (d) and the related requirements contained in points IS.I.OR.205 through IS.I.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.I.OR.205 and reviewed and approved by its competent authority.

ISO/IEC 27001 mapping

4.1 Understanding the organization and its context

Part-IS particularity

This is an "derogation" for organisations falling under the applicability of Article 2 of the regulation. This process is independent from an ISO/IEC 27001 certification process.

Guidance for Part-IS implementation

If an organisation, which already has an established ISMS according to ISO/IEC 27001 decides to embark on this process, the full implementation of Part-IS into the ISMS may go on hold until the decision of the competent authority is made.

To demonstrate that an organisations 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 existing risk assessment methodology according ISO/IEC 27001 chapter 6.1.2 may be used if the methodology is enhanced with a focus of impact on safety. On the other hand, an existing risk assessment methodology used by the existing safety management system (SMS) could be enhanced by addressing potential information security risks.

Anyhow, the competent authority responsible for the organisation will determine, which process and methodology shall be used,

This demonstration shall be at least verified and reassessed at regular intervals and as a mandatory part of the organisation´s change process. In case of any doubt about the conclusion, the appropriate Civil Aviation Authority must be contacted.

Note 1: The process to apply for a derogation according IS.OR.200(e) and the evidence needed will be defined by the national competent authority. Additional guidance is available at European level

Note 2: It is unlikely that an organisation falling under article 2 of the regulation and running an ISMS according to ISO/IEC 27001 will take use of this option.

An example could be a large (non-aviation) production company with a small unit for aviation-certified (Form 1 issued) non-critical parts for non ELA2 aircraft.

4.10 IS.OR.205 (a) Information security risk assessment

Requirement

(a) The organisation shall identify all 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).

ISO/IEC 27001 mapping

4.3 Determining the scope of the information security management system

6.1.2 Information security risk assessment

Part-IS particularity

This requirement of Part-IS is in line with ISO/IEC 27001, however ISO/IEC 27001 allows a more open focus, whereas Part-IS puts the focus on safety already from the element's identification stage.

In addition, all implementation rulesdomain-specific implementing regulations (namely ORO.GEN.200 (a) (3), ORA.GEN.200 (a) (3), CAMO.A.200 (a) (3), 145.A.200 (a) (3), 21.A.139 (b) (1), 21.A.239 (c) (3), ATM/ANS.OR.D.010 (b) (1), ATCO.OR.C.001 (c), ADR.OR.C.005 (b) (4), UAS.LUC.030 (2) (e)) of Reg. (EU) 2018/1139 require a risk assessment system, where information security can be integrated.

Guidance for Part-IS implementation

AMC1 IS.I.OR.205(a) explains that when conducting an information security risk assessment, the organisation should ensure that each relevant aviation safety impact is identified and included in the ISMS scope, which might not be the case when using ISO/IEC 27001.

On the other hand, an ISO/IEC 27001 ISMS focused in its security risk assessment mainly on the business impact of infringement on Confidentiality, Integrity and Availability, their risks and the impact on assets (e. g. loss of IT infrastructure, breach of data).

This means that, starting from an ISMS based on ISO/IEC 27001, a complementary analysis has to be made to **take into account all the elements related to aviation safety**.

To bridge the two approaches of Safety Management Systems (SMS) and ISMS, an identified information security risk may be entered as a "cause" or "contributing event" in the aviation safety focused risk assessment required by the "domain" specific implementing regulation. The figure in GM1.IS.OR.205(c) gives a good indication of how this bridge could be builtbuilt.

Example: "GNSS-Jamming/Spoofing" is nowadays a common information security threat with a direct impact on flight safety.

See also EASA SIB 2022-02R3:

Global Navigation Satellite System Outages and Alterations | EASA (europa.eu)

Also infringing on the integrity of flight preparation (e. g. corruption of an aircraft weight & balance sheet) can have a direct impact on aviation safety.

Similarly, the safety-related risk assessment can identify (external) causes , which may also be induced by an information security threat (intended vs. unintended).

One example is the accident of flight QF72 on Oct. 7th 2008 involving the Airbus A330 flight control primary computers, which was probably caused by an unintended event. In-flight upset - Airbus A330-303, VH-QPA, 154 km west of Learmonth, WA, 7 October 2008 | ATSB

4.11 IS.OR.205 (b) Information security risk assessment

Requirement

(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.

ISO/IEC 27001 mapping

4.1 Understanding the organisation and its context

4.3 Determining the scope of the information security management system

A5.19 Information security in supplier relationships

A5.21 Managing information security in the information and communication technology (ICT) supply chain

Part-IS particularity

IS.OR.205 (b) focuses on the identification of interfaces with the other organizations. ISO/IEC 27001 4.3 requires considering in point c) the interfaces and dependencies between activities performed by the organization and those that are performed by other organizations. So, there is more in Part-IS as required by ISO/IEC 27001, provided that the scope considered includes safety, as required by IS.OR.205 (a).

The Controls A5.19 and A5.21 are a profound foundation for the requirements of IS.OR.205 (b).

Guidance for Part-IS implementation

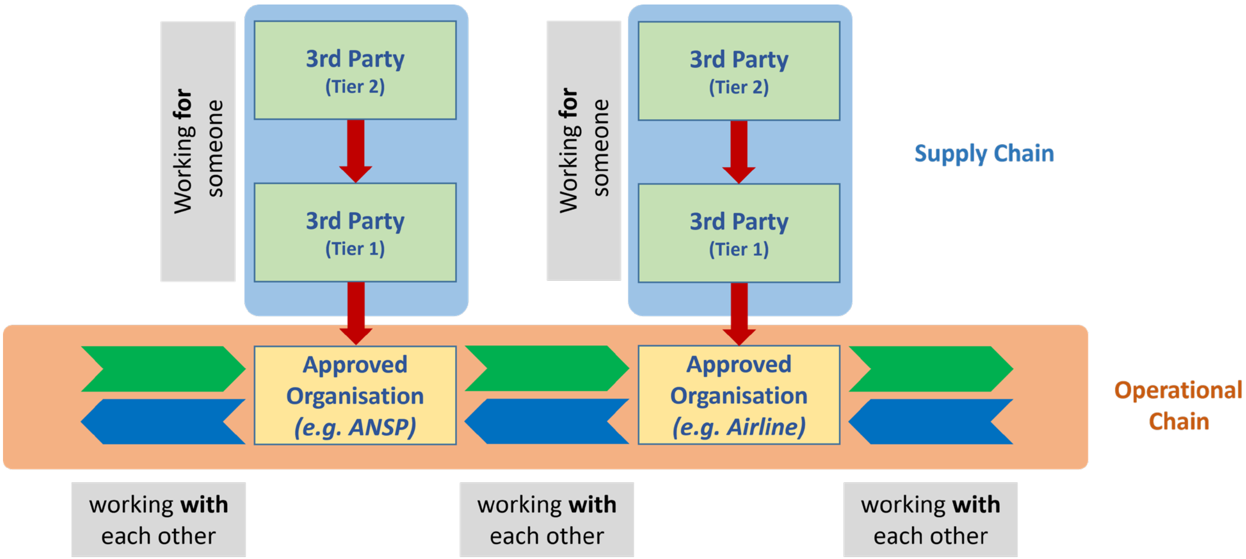
ISO/IEC 27001 A5.19 requires the identification of risks associated with the use of supplier's products or services. ISO 27002 A5.19 contains additional guidance in points f) to j) to manage the risk exposure.

ISO/IEC 27001 A5.21 requires the management of information security risks associated with the ICT products and services supply chain. ISO 27002 A5.21 contains additional guidance in points f), k), l) and m) to manage risks through the supply chain.

The Part-IS notion about interfaces and supply chain goes beyond the respective ISO/IEC 27001 notion. GM1 IS.I.OR.205(b) is requesting interfaced organizations to share information about mutual risks exposure (including all data flows) and urges organizations to use ED-201A for that. IS.OR.205 (c) also requires accounting for information acquired by interfaced organisations, which underlines the two-way nature of the considerations. Particular attention should be paid to the Part-IS intent to protect so-called "Functional Chains". The notion is that while organisations may to protect themselves well enough, interfaces between organisations may pose risks to each chain when unaccounted for.

Functional Chain Concept

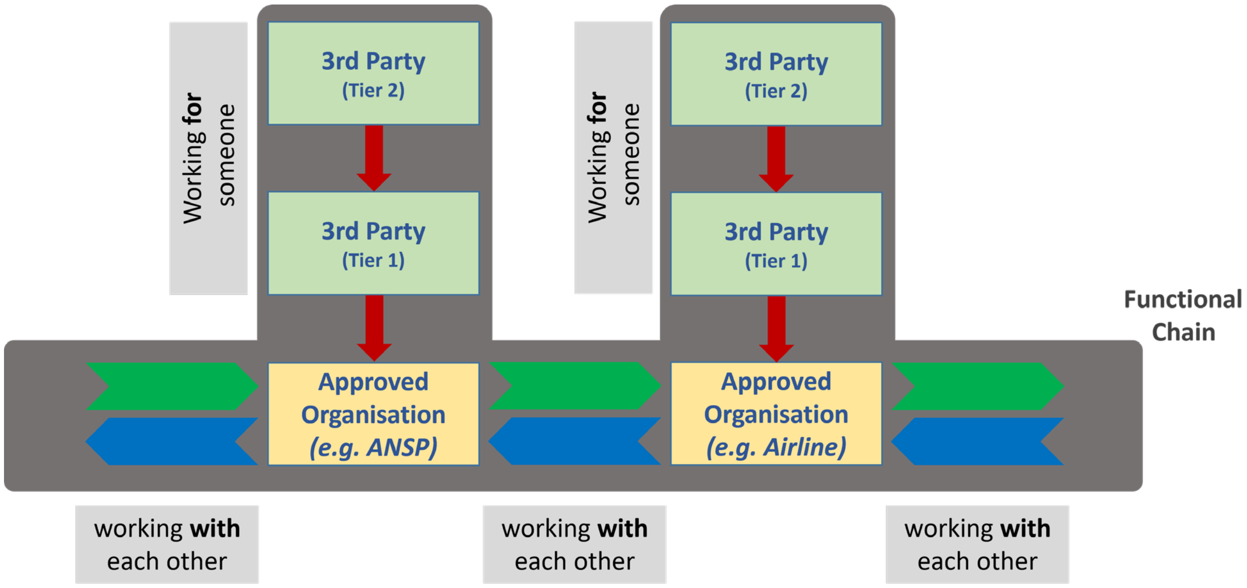
The origin of the Functional Chain concept lies in the realization, that aviation is considered a "System-of-Systems", with its participants (systems) interacting with each other according to a hierarchical set of rules and policies, as established by ICAO and its Contracting States. Hence, unlike in a **supply chain**, where one organization supplies products or services to another, the **operational chain** is based upon a collaborative approach to address operational tasks and risks to safety, security, and capacity and efficiency of air navigation.



The organizations that make the operational chain are the **organizations that hold an approval** to operate by their appropriate civil aviation authority. A non-exhaustive list holding an approval includes airports, airlines, aircraft or engine manufacturers, some aircraft equipment providers, air navigation service providers, maintenance repair organizations, approved training organizations, etc. The civil aviation authorities (CAA) themselves are also part of operational chains.

GM1 IS.I.OR.205 (b) differentiates between organisations that are subject to Part-IS from other organisations that are not subject to Part-IS when considering the interfaces. Within the scope of article 2 of the Part-IS regulations the organizations being part of the "operational chain" are only those organizations that are subject to Part-IS. The other organizations are considered in the context of "supply chain". Their interfaces could be treated as laid down in ISO/IEC 27001 controls A5.19 to A5.23.

The **functional chain** is integrating the operational chain and the supply chain. The rationale behind the functional chain approach is to ensure that the interfaces between organisations are adequately protected in order to prevent unwanted transfer of risks and to minimize expansion of the attack surface, while the organisations need to continue managing their own risks effectively. By securing these interfaces and maintaining strong internal risk management, overall safety risks are minimised.



On the diagrams, both, the green and blue flow, depict the operational information flows between parties working with each other. The organization sending the information is the provider of the information, and the one receiving it is the consumer of information. For example, a regulatory body (provider) issues safety instructions to an airline (consumer).

It is expected that both consumers and providers collaborate to make sure that the confidentiality, integrity, and availability of information are within acceptable boundaries for all consumers. This implies that it may be necessary to share risk assessment information and to collaborate at identified interfaces, and to provide feedback about issues or risks that the next organization in the chain cannot handle properly.

A few examples of existing Functional Chains and information exchange:

- An airport sending daily operational updates to airlines, like the runway in service.
- An Air Navigation Service Provider providing updates on arrival and departures to the airport.
- An airline providing technical feedbacks to an aircraft manufacturer about operational performance.
- A CAA (e.g., EASA) issuing Airworthiness Directives, for the benefit of airlines, aircraft maintenance organizations, and aircraft manufacturers.
- A local survey office (part of the supply chain) generating obstacle information, processed by CAA, service providers (like charts provider), operators (airline or ANSP), and aircraft, to be ultimately consumed by pilots.[2]

[2] The operational chain organizations in this example are the CAA, operators (airline or ANSP). Aircraft and pilots should be seen as part of the airline.

4.12 IS.OR.205 (c) Information security risk assessment

Requirement

(c) 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.I.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).

ISO/IEC 27001 mapping

6.1.2 Information security risk assessment

Part-IS particularity

IS.I.OR.205 (c) is the "heart" of Part-IS. ISO/IEC 27001 6.1.2 opens a “framework”, where the requirements of IS.OR.205 may fit in.

It has to be assured, that the risk management systems of the ISMS and those required by the SMS-regulations (see IS.OR.205 (a)) do NOT live independently, as there might be difficulties in connecting the two systems.

Guidance for Part-IS implementation

It requires that a proper risk assessment be made, taking into account the scope and interfaces described in 205(a) and 205(b). It has to be noted (see also GM1 IS. OR.205(c)) that IS.OR.205 does not require the use of any specific information security risk assessment framework, such as ISO31000, NIST or others to develop the risk assessment. ISO/IEC 27001 tends to lean towards using ISO 27005 as a risk assessment standard, however, it does not make it mandatory. The key point is, that the risk assessment carried out in the application of ISO/IEC 27001 6.1.2 does not necessarily consider safety risks, and may focus on different types of risks.

In respect to safety, conditions that may lead to safety consequences, are identified as ***hazards***. Their materialisation may be either directly triggered or caused by information security threats which have not successfully prevented. Information security can thus cause or contribute to a safety consequence in 4 different ways:

(1) It can act as a safety threat;
(2) it can have a negative effect on a safety barrier, rendering it less effective than before;
(3) it can directly trigger the materialisation of an already identified hazard; or
(4) can constitute a new, not yet identified, hazard, that can obviously also materialise.

By using e.g. the “bowtie-method” regarding information security, a “hazard” would be replaced by a “vulnerability”, which can be exploited resulting in information security consequences (e.g., lack or reduction of confidentiality, integrity, availability, authenticity properties). Hence, from a methodology perspective, both considerations are very similar and can be designed to interact (e. g. consequences of the “information security bowtie” may connect as causes of the “safety bowtie”)

<u>Guidance for organisations that are NOT required to operate an SMS, including safety risk management:</u>

Any ISO/IEC 27001 risk assessment shall be reviewed and revised by introducing safety impact (consequence) considerations.

Any risk matrix stemming from an ISO/IEC 27001 6.1.2 risk assessment is acceptable, provided it includes safety impacts (consequences), and the results remain within the limitations of ICAO Annex 19. If two different risk assessment schemes are used, they need to be linked accordingly.

<u>Guidance for organisations that are required to operate an SMS, including safety risk management:</u>

In most of the cases, where an organisation is falling under the domain specific implementing rules for SMS and is operating an ISMS under voluntary compliance with ISO/IEC 27001, it may operate two risk management systems, one for safety under the oversight of a competent authority, and one for information security. The latter may ultimately be certified by an ISO/IEC 27001 accredited body.

Each potential risk identified by the ISMS risk management shall be systematically assessed for its potential impact on safety. To establish the connection between the systems, the following approach should be used:

1. If a safety risk assessment is available, it should be able to provide its context and determined target likelihoods for acceptable information security risks to the information security risk assessment process. The context consists of the system architecture, including its preventative and mitigative barriers, the hazards assessed, and the safety risks identified. Based upon the information provided the information security risk assessment can be conducted. Modifications to the system architecture, or any modifications of properties of the preventative or mitigative barriers, as well as the achieved risk properties need to be communicated back to the safety risk assessment process. Based upon this communication, the safety risk assessment shall be updated. In other words: Mitigation measures put in place as a result of the information security risk assessment should also be considered as they may not only mitgate, but possibly also create a negative safety impact.
2. If a safety risk assessment is available, but the information security assessment process identifies a new hazard, that was previously unknown to the safety risk assessment, a full hazard assessment of all safety aspects shall be conducted to ensure that the safety risk assessment contains the “full picture” of the newly addressed hazard.
3. The cycling of the interacting safety risk and the information security risk assessments needs to be repeated until all acceptability requirements for all aspects are met.

4.13 IS.OR.205 (d) Information security risk assessment

Requirement

(d) The organisation shall review and update the risk assessment carried out in accordance with points (a), (b) and, as applicable, points (c) or (e), 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.

ISO/IEC 27001 mapping

6.3 Planning of changes

8.2 Information security risk assessment

Part-IS particularity

IS.I.OR.205 (d) is about the subsequent changes to the original risk assessment, due to a change of context or interfaces or knowledge about the risks, or lessons learnt. This is equivalent to ISO/IEC 27001 8.2. In both frameworks the reviews are planned and documented.

Guidance for Part-IS implementation

The same process as that already in place in an ISO/IEC 27001 context can be used to implement IS.OR.205 (d), provided that this process has been updated to accountinclude safety criteria evaluation of changes that trigger an unplanned update of the risk assessment.

Those organizations that have most experienced risk assessment updates at planned intervals will need to be proactive to trigger such updates more often in the situations listed in 205(d) (1), (2), (3), and (4) that could affect safety.

The triggering criteria and the process should be documented and tested before implementation, for example through table-top exercises.

The change management process is key to keep a management system in a solid and stable condition. Considering an established ISMS according to ISO/IEC 27001, the regular updates of the risk assessment based on changes and lessons learned should be effective. The essential focus, introduced by Part-IS is the “impact on safety”, which drives the update assessment.

A parallel process process is set out in all domain-specific implementing regulations (namely ORO.GEN.130, CAMO.A.130, 145.A.85, 21.A.147, 21.A.247, ATM/ANS.OR.A.040, ATCO.OR.B.015, ADR.OR.B.040, and UAS.LUC.070) of Reg. (EU) 2018/1139 for their changes which focuses on safety.

Without the “bridge” of Part-IS, both systems (ISMS and SMS) are implemented independently, often without considering interdependencies. Part-IS implies the need (and provides the opportunityopportunity) to interlink the systems to provide a common risk picture for the organisation, with a focus on safety, but also opening the horizon to information security.

4.14 IS.OR.205 (e) Information security risk assessment

Requirement

(e) By derogation from point (c), organisations required to comply with Subpart C of Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373 shall replace the analysis of the impact on aviation safety by an analysis of the impact on their services as per the safety support assessment required by point ATM/ANS.OR.C.005. This safety support assessment shall be made available to the air traffic service providers to whom they provide services, and those air traffic service providers shall be responsible for evaluating the impact on aviation safety.

ISO/IEC 27001 mapping

6.1.2 Information security risk assessment

Part-IS particularity

This Part-IS requirement is specific to organisations required to comply with Subpart C of Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373.

Guidance for Part-IS implementation

Those organisations falling under Subpart C of Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373, which are operating an ISO/IEC 27001:2022 conformed management system, use the mentioned "Safety Support Assessment" instead of the information security risk assessment requested in Part-IS.OR.205(c).

4.15 IS.OR.210 (a) Information security risk treatment

Requirement

(a) The organisation shall develop measures to address unacceptable risks identified in accordance with point IS.I.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.

ISO/IEC 27001 mapping

6.1.3 Information security risk treatment

8.3 Information security risk treatment

Part-IS particularity

IS.OR.210 (a) is about Information security risk treatment, which is widely covered by ISO/IEC 27001, its appendix A, and ISO/IEC 27002. IS.OR.210 (a) provides however some additional inputs related the risks that may have a safety impact.

Guidance for Part-IS implementation

ISO/IEC 27001 6.1.3 is about the definition of the risk treatment plan, while ISO/IEC 27001 8.3 deals with the implementation of the plan, and both are relevant.

ISO/IEC 27001 Annex A contains a list of possible information security controls, and therefore should also be used in addition to the already existing controls, to mitigate information security risks having an impact of safety. All the controls of Annex A are detailed in ISO/IEC 27002.

IS.I.OR.210 (a) specifies that the measures selected in the plan shall reduce the consequences on aviation safety associated with the materialisation of the threat scenario. This is in line with IS.I.OR.205 since the risk treatment phase is a consequence of the risk assessment phase and shall address all the risks that have been evaluated.

IS.I.OR.210 (a) also stipulates that those (protection) measures shall not introduce any new potential unacceptable risks to aviation safety.

This is an area, which is not directly covered neither by ISO/IEC 27001, nor ISOISO/IEC 27002. The requirement addresses the so called “side effects” when introducing measures into a system, (a well-known issue in software development which is also very relevant for information security measures). Preventive or mitigative measures specifically (e.g. physical security, access control) could lead to unintended side effects.

Also, the risk treatment of the identified risks should focus on addressing safety via the same linkage/integration of ISMS & Safety management.

4.16 IS.OR.210 (b) Information security risk treatment

Requirement

(b) The person referred to in point IS. 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.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.OR.205 (b) of any risk shared between both organisations.

ISO/IEC 27001 mapping

6.1.3.f Information security risk treatment

7.3 Awareness

9.3 Management review

A5.19 Information security in supplier relationships

A5.21 Managing information security in the ICT supply chain

Part-IS particularity

IS.OR.210 (b) is about the information of key personnel in the organization, about the risks, the corresponding threat scenarios and the security risk treatment measures, which result in specific controls covered by Annex A of ISO/IEC 27001 and ISO/IEC 27002. It partially covers IS.OR.210 (b), by the following requirement: obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

IS.OR.210 (b) has two specific requirements whichthat also have equivalent requirements in ISO/IEC 27001 and ISOISO/IEC 27002:

- Inform the accountable manager of the risk treatment plan – Which is a mandatory input to the management review.

- Inform the interfaced entities (the same as in IS.OR.205 (b)) of all risks shared with them - which is stated in A5.19 Guidance point l).

Guidance for Part-IS implementation

In addition to the risk owner's approval requested by ISO/IEC 27001 6.1.3.f, the organization will need to:

- Inform the accountable manager of the risk treatment plan: ISO/IEC 27001 9.3. f) defines "results of risk assessment and status of risk treatment plan" as mandatory input for the management review which is the vehicle to inform the accountable managers.

- Inform the interfaced entities (the same as in IS.OR.205 (b)) of all risks shared with them: ISOISO/IEC 27002 A5.21 states in point f) "defining rules for sharing of information and any potential issues and compromises between the organizations". GM1 IS.I.OR.205 (b) and ED-201A may also be used as a guidance for risk sharing.

4.17 IS.OR.215 (a) Information security internal reporting scheme

Requirement

(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.I.OR.230.

ISO/IEC 27001 mapping

A5.24 Information security incident management planning and preparation

A6.8 Information security event reporting

Part-IS particularity

Fully covered by the requirements of A5.24 and A6.8. However, the linkage to the external reporting scheme for the incidents with relation to safety (unsafe conditions) shall be established.

Guidance for Part-IS implementation

The linkage to the external reporting scheme for the incidents with relation to safety could be described under A5.5 (contact with authorities) in the ISO structure.

4.18 IS.OR.215 (b) Information security internal reporting scheme

Requirement

(b) That scheme and the process referred to in point IS.I.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.I.OR.205 and IS.I.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.

ISO/IEC 27001 mapping

A5.25 Assessment and decision on information security events

A5.26 Response to information security incidents

A5.27 Learning from information security incidents

A5.28 Collection of evidence

A8.8 Management of technical vulnerabilities

Part-IS particularity

Fully covered by the requirements of A5.25 to A5.28 and a connection to A8.8 with a need to focus on safety impacts.

Guidance for Part-IS implementation

The Requirements of the controls A8.8, A5.25 to A5.28 and the guidance in ISO 27002:2022 is comprehensive to fulfil the requirements of this paragraph.

According (b) (1) the impact on safety always needs to be assessed specifically.

AMC1 IS.I.OR.215 (a) & (b) shall be considered.

4.19 IS.OR.215 (c) Information security internal reporting scheme

Requirement

(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).

ISO/IEC 27001 mapping

A5.19 Information security in supplier relationships

A5.20 Addressing information security within supplier agreements

A5.21 Managing information security in the information and communication technology (ICT) supply chain

Part-IS particularity

To be covered under the procedures according A5.19 and A5.21 to be informed by the contracted organisation, as well as in the agreements under A5.20.

Guidance for Part-IS implementation

However, it depends, if the supplier also falls under Part-IS or not. In the latter case, the external reporting shall be done by the organisation contracting. GM1 IS.I.OR.215(c) provides guidance to implement the relationship with contracted organisations.

4.20 IS.OR.215 (d) Information security internal reporting scheme

Requirement

(d) The organisation shall cooperate on investigations with any other organisation that has a significant contribution to the information security of its own activities.

ISO/IEC 27001 mapping

A5.6 Contact with special interest groups

A5.20 Addressing information security within supplier agreements

A5.21 Managing information security in the information and communication technology (ICT) supply chain

A5.28 Collection of evidence

Part-IS particularity

The Requirements of the controls A5.20, A5.21 and A5.28 and the guidance in ISO 27002:2022 is comprehensive to fulfil the requirements of thisof this paragraph in terms of process, but Part-IS will require cooperation with a broader range of organizations.

Guidance for Part-IS implementation

As ISO/IEC 27001:2022 only focuses on the supply chain and Part-IS requires a broader focus, the process needs to be highlighted to other relevant stakeholders. This may be covered under A5.6. Nevertheless, ISO 27002 A5.19 has a clear statement under point (i) of the guidance.

See also the cooperation according to IS.OR.205 (c).

4.21 IS.OR.215 (e) Information security internal reporting scheme

Requirement

(e) The organisation may integrate that reporting scheme with other reporting schemes it has already implemented.

ISO/IEC 27001 mapping

A5.24 Information security incident management planning and preparation

A6.8 Information security event reporting

Part-IS particularity

Fully covered by the requirements of A5.24 and A6.8.

Guidance for Part-IS implementation

However, the linkage to the external reporting scheme for the incidents with relation to safety (unsafe conditions) shall be established. This could be described under A5.5 (contact with authorities) in the ISO structure.

4.22 IS.OR.220 (a) Information security incidents — detection, response & recovery

Requirement

(a) Based on the outcome of the risk assessment carried out in accordance with point IS.I.OR.205 and the outcome of the risk treatment performed in accordance with point IS.I.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.

ISO/IEC 27001 mapping

A5.24 Information security incident management planning and preparation

A5.25 Assessment and decision on information security events

A5.26 Response to information security incidents

A5.27 Learning from information security incidents

A5.28 Collection of evidence

A5.29 Information security during disruption

A7.5 Physical security monitoring

A8.16 Monitoring activities

Part-IS particularity

Fully covered by the requirements of A5.24, to A5.29, and A7.5 for physical security and A8.16 for technical monitoring.

Guidance for Part-IS implementation

The requirements of the controls (both reactive and proactive) mentioned above and the guidance in ISO 27002:2022 is comprehensive to fulfil the requirements of this paragraph. Again, the impact on safety needs to be assessed and measures shall be taken to ensure safety. Part-IS reflects to "unsafe conditions", which shall be mitigated to an acceptable level. A re-assessment of the risks affected by an incident or vulnerability identified is mandatory in Part-IS to ensure that no unacceptable risk appears through the incident/vulnerability.

Rem.: Due to historical reasons, information security and safety management are using different wording in explaining situations which are pretty the same. The term incident is used in a similar way (an event which already happened and infringing safety/security). A vulnerability in the sense of information security could be mapped to the term "hazard" in the area of safety (a situation identified, which is possible to happen, but has not happened so far).

AMC1.IS.OR.220 (a) shall be applied.

4.23 IS.OR.220 (b) Information security incidents — detection, response & recovery

Requirement

(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.I.OR.205(a).

ISO/IEC 27001 mapping

A5.26 Response to information security incidents

A5.29 Information security during disruption

A7.5 Physical security monitoring

A8.8 Management of technical vulnerabilities

Part-IS particularity

Fully covered by the requirements of A5.26, and A5.29.

Guidance for Part-IS implementation

The Requirements of the control A5.26 and the guidance in ISO 27002:2022 is comprehensive to fulfil the requirements of this paragraph. IS.OR.220 deals mainly with incidents, IS.OR.220 (b) related to information security events, which might be more generic.

4.24 IS.OR.220 (c) Information security incidents — detection, response & recovery

Requirement

(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.I.OR.205(a) within a recovery time previously defined by the organisation.

ISO/IEC 27001 mapping

A5.26 Response to information security incidents

A5.29 Information security during disruption

Part-IS particularity

This requirement is covered by the requirements of A5.26, and A5.29, with the difference that the recovery here is not intendedto continuously ensure confidentiality, integrity, availability and integrity, but is intended to maintain or return to an acceptable level of safety.

In addition, some "domain specific" implementation rules (e.g. ARO.GEN.200, ATM/ANS.OR.A.070, ADR.OR.B.070) of Reg. (EU) 2018/1139 require emergency response planning and/or contingency planning, where information security should be integrated.

Guidance for Part-IS implementation

Coupled with the requirements of controls A5.26 and A5.28 and the guidance in ISOISO/IEC 27002:2022, AMC1.IS.OR.220 (c) should be applied in order to revert as quickly as possible to a safe state.

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

Requirement

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

(1) identify the root cause or causes of, and contributing factors to, the non-compliance;

(2) define a corrective action plan;

(3) demonstrate the correction of the non-compliance to the satisfaction of the competent authority.

(b) The actions referred to in point (a) shall be carried out within the period agreed with the competent authority.

ISO/IEC 27001 mapping

10.2 Non-conformity and corrective action

Part-IS particularity

This requirement does not have a direct representation in ISO/IEC 27001. However, most domain-specific implementing regulations (namely ORO.GEN.150, ORA.GEN.150, CAMO.A.150, 145.A.95, 21.A.158, 21.A.258 ATM/ANS.OR.A.055, ATCO.OR.B.030, ADR.OR.C.020) of Reg. (EU) 2018/1139 require a similar function, which may be used.

Guidance for Part-IS implementation

This issue is specifically not covered by the ISO/IEC 27001:2022 requirements. However, a similar requirement is laid downset out in the domain-specific "safety" implementing rules of Reg. (EU) 2018/1139as defined above.

See also AMC1.IS.OR.225.

4.26 IS.OR.230 Information security external reporting scheme

Requirement

(a) The organisation shall implement an information security reporting system that complies with the requirements laid down in Regulation (EU) No 376/2014 and its delegated and implementing acts if that Regulation is applicable to the organisation.

(b) Without prejudice to the obligations of Regulation (EU) 376/2014, the organisation shall ensure that any information security incident or vulnerability, which may represent a significant risk to aviation safety, is reported to their competent authority. Furthermore:

(1) 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;

(2) Where such an incident or vulnerability affects a system or constituent used by the organisation, the organisation shall report it to the organisation responsible for the design of the system or constituent.

(c) The organisation shall report the conditions referred to in point (b) as follows:

(1) a notification shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, as soon as the condition has been known to the organisation.

(2) a report shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, as soon as possible, but not exceeding 72 hours from the time the condition has been known to the organisation, unless exceptional circumstances prevent this.
The report shall be made in the form defined by the competent authority and shall contain all relevant information about the condition known to the organisation;

(3) a follow-up report shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, providing details of the actions the organisation has taken or intends to take to recover from the incident and the actions it intends to take to prevent similar information security incidents in the future.
The follow-up report shall be submitted as soon as those actions have been identified, and shall be produced in the form defined by the competent authority.

ISO/IEC 27001 mapping

A5.5 Contact with authorities

Part-IS particularity

This requirement is not directly addressed in ISO/IEC 27001.

However, most domain-specific implementing regulations (e.g. ORO.GEN.160, ORA.GEN.160, CAMO.A.160, 21.A.139 (c) (6), 21.A.239 (c) (6), ATM/ANS.OR.A.065, ATCO.OR.B.040, ADR.OR.C.030) of Reg. (EU) 2018/1139 require also an external occurrence reporting system, where information security will be integrated.

Guidance for Part-IS implementation

This issue is specifically not directly covered by ISO/IEC 27001 requirements. Consider also the reporting requirement if the organisation falls under the NIS directive.

AMC1 IS.I.OR.230 (a) & (b) and AMC1 IS.I.OR.230 (c) should be considered.

4.27 IS.OR.235 (a) Contracting of information security management activities

Requirement

(a) The organisation shall ensure that when contracting any part of the activities referred to in point IS.I.OR.200 to other organisations, the 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.

ISO/IEC 27001 mapping

A5.19 Information security in supplier relationships

A5.21 Managing information security in the information and communication technology (ICT) supply chain

A5.22 Monitoring, review and change management of supplier services

Part-IS particularity

ISO/IEC 27001 controls A5.19, A5.21 and A5.29 may cover this requirement. The difference in the requirements of IS.OR.235 is, that it is limited to those activities directly related to the ISMS (e. g. internal audits, consultancy for risk assessments, ….).

In addition, all “domain specific” implementation rules (e.g. ORO.AOC.110, ORA.GEN.205, CAMO.A.205, 145.A.205, 21.A.139 (d) (1), 21.A.239 (d) (3), ATM/ANS.OR.B.020, ATCO.OR.C.005, ADR.OR.D.010,) of Reg. (EU) 2018/1139 require procedures to deal with contracted activities in a wider scope, where information security should be integrated.

Guidance for Part-IS implementation

This requirement relates only to ISMS activities (e.g., internal audits, risk assessments), not to those activities not directly related to ISMS itself (e. g. hardware, software, IT, OT).

The difference in the requirements of IS.OR.235 is, that it is limited to those activities directly related to the ISMS (e. g. internal audits, consultancy for risk assessments, ….). The controls in ISO/IEC 27001 do not exclude those kinds of services, but sometimes it will not be in the focus of the organisation.

Therefore, there is no need to establish an independent system for those contractors mentioned IS.OR.235 (a). The list of suppliers should be reviewed to ensure, that the suppliers providing the services mentioned in IS.OR.235 are covered.

4.28 IS.OR.235 (b) Contracting of information security management activities

Requirement

(b) The organisation shall ensure that the competent authority can have access upon request to the contracted organisation to determine continued compliance with the applicable requirements laid down in this Regulation.

ISO/IEC 27001 mapping

A5.20 Addressing information security within supplier agreements

Part-IS particularity

Access given to the authority is not covered in ISO/IEC 27001

In addition, most implementation rulesdomain-specific implementing regulations (namely ORO.GEN.140, ORA.GEN.140, CAMO.A.140, 145.A.140, 21.A.9, ATCO.OR.B.025, ADR.OR.C.015, and UAS.LUC.090) of Reg. (EU) 2018/1139 require access for the authority, where information security should be integrated.

Guidance for Part-IS implementation

For organisations, falling under Part-IS, the access to the competent authority is mutually granted. If the contracting organisation is approved by an authority of another Member State, the different competent authorities will arrange themselves according their authority procedures (e.g. Reg. 965/2012 ARO.GEN.300 (e).

For contracted organisations not falling under Part-IS, GM1 IS.I.OR.235 (b) provides the content to be introduced either in the "General Term and Conditions of Trade" of the contracting organisation, or if standard General Terms and Conditions are used (e. g. for COTS-products), the content of the GM shall be arranged on a contractual basis (e. g. through a side letter).

AMC1.IS.OR.235 (b) shall be applied in conjunction with ISO/IEC 27001 A5.20.

4.29 IS.OR.240 (a) + (e) Personnel requirements

Requirement

(a) The accountable manager of the organisation designated in accordance with the Regulation (EU) No 1321/2014, Regulation (EU) No 965/2012, Regulation (EU) No 1178/2011, Regulation (EU) 2015/340, Regulation (EU) 2017/373 or Regulation (EU) 2021/664 as applicable referred to in Article 2(1) of this Regulation shall have corporate authority to ensure that all activities required by this Regulation can be financed and carried out. That person shall:

(1) ensure that all necessary resources are available to comply with the requirements of this Regulation;

(2) establish and promote the information security policy referred to in point IS.I.OR.200(a)(1);

(3) demonstrate a basic understanding of this Regulation.

(e) The accountable manager or the common responsible person referred to in (d) shall have corporate authority to establish and maintain the organisational structures, policies, processes and procedures necessary to implement point IS.I.OR.200.

ISO/IEC 27001 mapping

5.1 Leadership and commitment

5.3 Organizational roles, responsibilities and authorities

7.1 Resources

A5.2 Information security roles and responsibilities

A5.3 Management responsibilities

Part-IS particularity

ISO/IEC 27001 does not require a specific role such as the “accountable manager”.

However, all domain-specific implementing regulations (namely ORO.GEN.210 (a), ORA.GEN.210 (c), CAMO.A. 305 (a), 145.A.30 (a), 21.A.145 (a), 21.A.245 (a), ATM/ANS.OR.B.020 (a), ATCO.OR.C.010 (a), ADR.OR.D.005 (b) (1), UAS.LUC.030 (2) (a)) of Reg. (EU) 2018/1139 require similar assignments, but related to safety.

Guidance for Part-IS implementation

The implementation of the requirements of IS.OR.240 (a) may be spread into the implementation of ISO/IEC 27001 requirements mentioned above provided the accountable manager role is clearly defined and meets the requirements in (a).

The requirement of (a) (3) shall be set in line with the roles in A5.2 (where an accountable manager is not foreseen). However, the measures in control A6.3 should be used to ensure the competency of the accountable manager (IS.OR.240 (a) (3)).

4.30 IS.OR.240 (b) + (c) Personnel requirements

Requirement

(b) The accountable manager shall appoint a person or group of persons to ensure that the organisation complies with the requirements of this Regulation, and shall define the extent of their authority. That person or group of persons shall report directly to the accountable manager, and shall have the appropriate knowledge, background and experience to discharge their responsibilities. It shall be determined in the procedures who deputises for a particular person in the case of lengthy absence of that person.

(c) The accountable manager shall appoint a person or group of persons with the responsibility to manage the compliance monitoring function referred to in point IS.I.OR.200 (a) (12).

ISO/IEC 27001 mapping

5.3 Organisational roles, responsibilities and authorities

7.1 Resources

A5.2 Information security roles and responsibilities

A5.3 Segregation of duties

Part-IS particularity

Regarding (c), all “domain specific” implementation rules (namely ORO.GEN.210 (b), ORA.GEN.210 (b), CAMO.A.305 (b), 145.A.30, 21.A.145, 21.A.245, ATM/ANS.OR.B.005 (a) (1), ATCO.OR.C.010, ADR.OR.D.015 (c), UAS.LUC.030 (2) (d)) of Reg. (EU) 2018/1139 require all those assignments, but related to safety.

Guidance for Part-IS implementation

The implementation of the requirements of A5.2 and A5.3 should be used to integrate the needs of IS.OR.240 (b) and (c).

This issue is covered in A5.2, but also A5.3 may apply. However, similar requirements for the "safety roles" are laid down in the domain specific "safety" implementing rules of Reg. (EU) 2018/1139.

AMC1 IS.I.OR.240 (b) shall be applied.

4.31 IS.OR.240 (d) Personnel requirements

Requirement

(d) Where the organisation shares information security organisational structures, policies, processes and procedures with other organisations or with areas of their own organisation which are not part of the approval or declaration, the accountable manager may delegate its activities to a common responsible person.
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.

ISO/IEC 27001 mapping

4.3 Determining the scope of the information security management system

A5.2 Information security roles and responsibilities

A5.3 Segregation of duties

Part-IS particularity

The implementation of the requirements of A5.2, A5.3 and the guidance of ISO 27002 allows the delegation of responsibility within organisations.

Guidance for Part-IS implementation

This option might be useful for large entity or groups, where the ISMS is implemented as an “umbrella function” over a group of organisations, where not all of them will fall under Part-IS.

The implementation of a “group CISO” or an enterprise-wide ISMS could make use of this option in Part-IS.

Nevertheless, the common responsible person has to fulfil the competency requirements of IS-OR.240 (a) (3). This might be relevant in cases where the other activities of the organisation or group are not related to aviation.

4.32 IS.OR.240 (f) Personnel requirements

Requirement

(f) The organisation shall have a process in place to ensure that they have sufficient personnel on duty to carry out the activities covered by this Annex.

ISO/IEC 27001 mapping

7.1 Resources

Part-IS particularity

The implementation of the requirements of 7.1 should be used.

In addition, some domain-specific implementing regulations (e.g. ORO.GEN.210 (c), ORA.GEN.210 (c), CAMO.A.305 (d), 21.A.245 (e) (1), ATCO.OR.C.010 (c), ADR.OR.D.015 (d)) of Reg. (EU) 2018/1139 require a capacity planning, but related to safety.

Guidance for Part-IS implementation

A systematic capacity planning of human resources is a key element of any management system. Therefore, such a process should have been established in an ISMS. The possible additional requirement induced by Part-IS shall be assessed and the capacity planning shall be updated accordingly.

The targeted safety levels set in the safety/cyberrisk assessment shall never be jeopardized by a lack of ressources, even temporarily.

AMC1 IS.OR.240 (f) should be considered.

4.33 IS.OR.240 (g) Personnel requirements

Requirement

(g) The organisation shall have a process in place to ensure that the personnel referred to in point (f) have the necessary competence to perform their tasks.

ISO/IEC 27001 mapping

7.2 Competency

A6.3 Information security awareness, education and training

Part-IS particularity

The implementation of the requirements of 7.2 and A6.3 are sufficient to cover the requirement.

In addition, most domain-specific implementing regulations (e.g. ORO.GEN.210 (d), ORA.GEN.210 (d), CAMO.A.305 (c), 145.A.30 (e), 21.A.145 (d), 21.A.245 (e) (1), ATM/ANS.OR.B.005 (a) (6), ATCO.OR.C.010 (c), ADR.OR.D.015 (f)) of Reg. (EU) 2018/1139 require an adequate competency, but related to safety.

Guidance for Part-IS implementation

A systematic competency management process of staff is a key element of any management system. Therefore, such a process should have been established in the ISMS. The possible additional requirement induced by Part-IS shall be assessed and the competency requirements shall be updated.

AMC1 IS.OR.240 (g) should be considered.

4.34 IS.OR.240 (h) Personnel requirements

Requirement

(h) The organisation shall have a process in place to ensure that personnel acknowledge the responsibilities associated with the assigned roles and tasks.

ISO/IEC 27001 mapping

A6.2 Terms and conditions of employment

Part-IS particularity

The requirements of A6.2 would be sufficient to integrate the requirement.

Guidance for Part-IS implementation

OR.240 (h) is (at least partially) covered by ISO/IEC 27001 A.6.2 "The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security." and A.6.4 "disciplinary process" (see "Just Culture").

It depends on the organisational culture, if job descriptions or role assignments need to be formally acknowledged. In many organisations, the assigned jobs and roles are mutually acknowledged by performing the tasks assigned.

4.35 IS.OR.240 (i) Personnel requirements

Requirement

(i) 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.

ISO/IEC 27001 mapping

A5.19 Information security in supplier relationships

A6.1 Screening

A7.2 Physical entry

A8.3 Information access restriction

A8.5 Secure authentication

Part-IS particularity

The implementation of the requirements of A5.19, A6.1, A7.2, A8.3 and A8.5 might be sufficient controls to cover this requirement for personnel of the organisation, as well as for contractors and suppliers.

Guidance for Part-IS implementation

All the controls established in an ISO/IEC 27001conformed compliant ISMS are designed to ensure the confidentiality and integrity of information. The implementation of those controls will provide sufficient protection to ensure compliance with this requirement.

AMC1 IS.OR.240 (i) should be considered.

4.36 IS.OR.245 (a) Record-keeping

Requirement

(a) The organisation shall keep records of its information security management activities

(3) The organisation shall ensure that the following records are archived and traceable:

(i) any approval received and any associated information security risk assessment in accordance with point IS.I.OR.200(e;)

(ii) contracts for activities referred to in point IS.I.OR.200(a)(9);

(iii) records of the key processes referred to in point IS.I.OR.200(d);

(iv) records of the risks identified in the risk assessment referred to in point IS.I.OR.205 along with the associated risk treatment measures referred to in point IS.I.OR.210;

(v) records of information security incidents and vulnerabilities reported in accordance with the reporting schemes referred to in points IS.I.OR.215 and IS.I.OR.230;

(vi) records of those information security events which may need to be reassessed to reveal undetected information security incidents or vulnerabilities.

(4) The records referred to in point (1)(i) shall be retained at least until 5 years after the approval has lost its validity.

(5) The records referred to in point (1)(ii) shall be retained at least until 5 years after the contract has been amended or terminated.

(6) The records referred to point (1)(iii), (iv) and (v) shall be retained at least for a period of 5 years.

(7) The records referred to in point (1)(vi) shall be retained until those information security events have been reassessed in accordance with a periodicity defined in a procedure established by the organisation.

ISO/IEC 27001 mapping

7.5 Documented information

A5.9 Inventory of information and other associated assets

A5.13 Labelling of information

A8.10 Information deletion

A8.13 Information backup

Part-IS particularity

Record keeping and retention is an inherent part of the document control system under 7.5 of ISO/IEC 27001. The controls A5.9, A5.13, A8.10 and A813 also apply.

In addition, all domain-specific implementing regulations (e.g. ORO.GEN.220, ORA.GEN.220, CAMO.A.220, 145.A.55, 21.A.5, ATM/ANS.OR.B.005 (b), ATCO.OR.C.010 (e), ADR.OR.D.005 (c), UAS.LUC.030 (2) (g)) of Reg. (EU) 2018/1139 require record keeping, but related to safety.

Guidance for Part-IS implementation

Chapter 7.5.1 b) states that the ISMS shall include "documented information determined by the organization as being necessary for the effectiveness of the information security management system.", This includes the records defined in IS.OR.245 (a) (1). Chapter 7.5.3 requires under f) also document control for retention and disposition. Part-IS requirements shall be integrated into the existing system, especially the minimum duration of record-keeping of 5 years.

The minimum set of records, as defined in OR.245 (a) (1) should be covered in the inventory of assets. For the coverage, the content of GM1 IS.I.OR.245 also applies.

As records are not only information assets, the requested "record retention policy may be integratedintegrated into a wider policy as recommended by ISO 27002:2022 above.

AMC1 IS.I.OR.245 (a) (1) (vi) & (a) (5) should be implemented.

4.37 IS.OR.245 (b) Record-keeping

Requirement

(b) The organisation shall keep records of qualification and experience of its own staff involved in information security management activities

(1) The personnel's qualification and experience records shall be retained for as long as the person works for the organisation, and for at least 3 years after the person has left the organisation.

(2) Members of the staff shall, upon their request, be given access to their individual records. In addition, upon their request, the organisation shall provide them with a copy of their individual records on leaving the organisation.

ISO/IEC 27001 mapping

7.5 Documented information

A5.9 Inventory of information and other associated assets

A5.10 Acceptable use of information and other associated assets

A5.13 Labelling of information

A5.34 Privacy and protection of personal identifiable information (PII)

A8.10 Information deletion

A8.13 Information backup

Part-IS particularity

Record keeping and retention is an inherent part of the document control system under 7.5 of ISO/IEC 27001. The controls A5.9, A5.13, A8.10 and A813 will also apply and due to GDPR issues specifically also A5.10 and A5.34.

In addition, all domain-specific implementing regulations (e.g. ORO.GEN.220, ORA.GEN.220, CAMO.A.220, 145.A.55, 21.A.5, ATM/ANS.OR.B.005 (b), ATCO.OR.C.010 (e), ADR.OR.D.005 (c), UAS.LUC.030 (2) (g)) of Reg. (EU) 2018/1139 require record-keeping, but related to safety personnel.

Guidance for Part-IS implementation

Chapter 7.5.1 b) states that the ISMS shall include “documented information determined by the organization as being necessary for the effectiveness of the information security management system.” This includes the records defined in IS.OR.245 (a) (1). Chapter 7.5.3 requires under f) also document control for retention and disposition. Part-IS requirements shall be integrated into the existing system, especially the minimum duration of record-keeping of 5 years.

However, there is no retention duration specified in ISO/IEC 27001, whereas Part.IS OR.245 (a) specifies 3 years after the person has left the organisation.

As these records fall under the GDPR Regulation, each organisation has to ensure, that they are handled accordingly. It is recommended to use the procedures not only for records related to ISMS, but to the entire HR personnelpersonal files of the staff.

4.38 IS.OR.245 (c) Record-keeping

Requirement

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

ISO/IEC 27001 mapping

7.5 Documented information

A5.13 Labelling of information

Part-IS particularity

Record keeping and retention is an inherent part of the document control system under 7.5 of ISO/IEC 27001 as well as the control A5.13.

Guidance for Part-IS implementation

Chapter 7.5.3 requires under a) that “it is available and suitable for use, where and when it is needed”. Part-IS requirements shall be integrated into the existing system.

ISO 27002:2022 A5.13 states: "Procedures for information labelling should cover information and other associated assets in all formats.”, therefore the Part-IS requirement is fulfilled with control A5.13.

A series of AMC material of the implementing regulations regarding safety (e. g. AMC1 ARA.GEN.220 (a), AMC1 145.A.55) state requirements to cover this issue.

4.39 IS.OR.245 (d) Record-keeping

Requirement

(d) Records shall be stored in a manner that ensures protection from damage, alteration and theft, with information being identified, when required, according to its security classification level. The organisation shall ensure that the records are stored using means to ensure integrity, authenticity and authorised access.

ISO/IEC 27001 mapping

7.5 Documented information

A5.10 Acceptable use of information and other associated assets

A5.12 Classification of information

A5.33 Protection of records

A8.12 Data leakage prevention

Part-IS particularity

Record keeping and retention is an inherent part of the document control system under 7.5 of ISO/IEC 27001. The controls A5.10, A5.12, A5.33 and A8.12 will also apply.

Guidance for Part-IS implementation

Chapter 7.5.3 requires under d) that "storage and preservation, including the preservation of legibility". Part-IS requirements shall be integrated into the existing system.

The application of A5.33 and A8.12 has a strong relationship to A7.5 (Protecting against physical and environmental threats), A7.10 (Storage media), A8.3 (Information access restriction), A8.13 (Information backup), A8.14 (Redundancy of information processing facilities), A8.15 (Logging), A8.17 (Clock synchronization) and A8.24 (Use of cryptography).

A series of AMC material of the implementing regulations regarding safety (e. g. AMC1 ARA.GEN.220 (a), AMC1 145.A.55) state requirements to cover this issue.

4.40 IS.OR.250 (a) Information security management manual (ISMM)

Requirement

(a) The organisation shall make available to the competent authority an information security management manual (ISMM) and, where applicable, any referenced associated manuals and procedures, containing:

(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.

ISO/IEC 27001 mapping

7.5 Documented information

A5.13 Labelling of information

Part-IS particularity

Document control is an inherent part of the ISMS under 7.5 of ISO/IEC 27001. The control A5.13 is also an “anchor point” for this requirement. ISO 27001 does not specifically request a document called “information security management manual”, made available to the authority.

Guidance for Part-IS implementation

Chapter 7.5.1 b) states that the ISMS shall include “documented information determined by the organisation as being necessary for the effectiveness of the information security management system,” which will allow the inclusion of the ISMS manual in the documentation.

Part-IS requires a specific ISMS manual, made available to the competent authority.

It shall be made clear to the competent authority, which a set of documented information constitutes the "approved manual". The document "statement of applicability" (SOA), mandatory for all ISO/IEC 27001 certified organisations may be helpful (e.g. by adding an additional column to label specific documents as part of a “virtual” ISMS-Manual,). GM1 IS.I.OR.250(a) is also opening this way forward).

It has to be ensured, that all information listed in IS.OR.250 (a) is covered.

4.41 IS.OR.250 (b) +(c) Information security management manual (ISMM)

Requirement

(b) 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.

(c) Amendments to the ISMM shall be managed in a procedure established by the organisation. Any amendments that are not included within the scope of this procedure and any amendments related to the changes referred to in point IS.I.OR.255 (b) shall be approved by the competent authority.

ISO/IEC 27001 mapping

7.5 Documented information

A5.5 Contact with authorities

Part-IS particularity

Document control is an inherent part of the ISMS under 7.5 of ISO/IEC 27001.

In addition, most implementation rulesdomain-specific implementing regulations (namely ORO.MLR.100, ORA.ATO.130, CAMO.A.300, 145.A.70, 21.A.43, 21.A.243, ATM/ANS.OR.B.035, ADR.OR.E.005, and UAS.LUC.040) of Reg. (EU) 2018/1139 require a similar procedure for their manuals.

Guidance for Part-IS implementation

It is recommended to use the same procedure, which is implemented for the “safety-regulations” (see above) also for the approval, update and communication processes with the competent authority.

Many organisations have their documented information available via document management systems (e.g. MS SharePoint). The access for the competent authority to these systems has to be managed in accordance with the rules of any other external access in respect of A5.15, A5.18, A6.6, A7.9, A8.3, A8.7, A8.11, and A8.24.

4.42 IS.OR.250 (d) Information security management manual (ISMM)

Requirement

(d) 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.

ISO/IEC 27001 mapping

7.5 Documented information

Part-IS particularity

This requirement (which is not mandatory) has no specific counterpart in ISO/IEC 27001. However, by following the ISO “Annex SL” structure ISO/IEC 27001 is enabling an easy integration of other management system standards.

Guidance for Part-IS implementation

There is a tendency in the aviation industry to integrate different management systems, depending on the structure of the organisation. Some national documentation will support this trend.

Example: Extract from the Austrian State Safety Programme

4.2.1.2.3 The Possibility to develop an Organisation’s Management Manual

As stated above in “Duplicated Definitions (undesired redundancies)” the aviation industry suffers from duplicated definitions in the manuals. The EU Regulations regarding “Organisations’ Requirements” permit to avoid duplicated definitions of organisational aspects. This approach provides the chance for an enormous simplification especially for combined organisations. For combined organisations, it is recommended to develop a controlling manual describing the general organisation, responsibilities, procedures, etc., which are common and valid also for other manuals / documents of the organisation. Whereas specific topics related to aircraft operations, pilot training, aircraft maintenance for example still remain documented in the respective manuals (e.g. MOE, CAME, TM, OM, FSTD) as required by the respective Part. The controlling manual may be named as Organisation Management Manual (OMM), as this OMM is describing the organisation as a whole. This is also in line with the description and guidelines as published in the “Foreign ATO” by EASA.

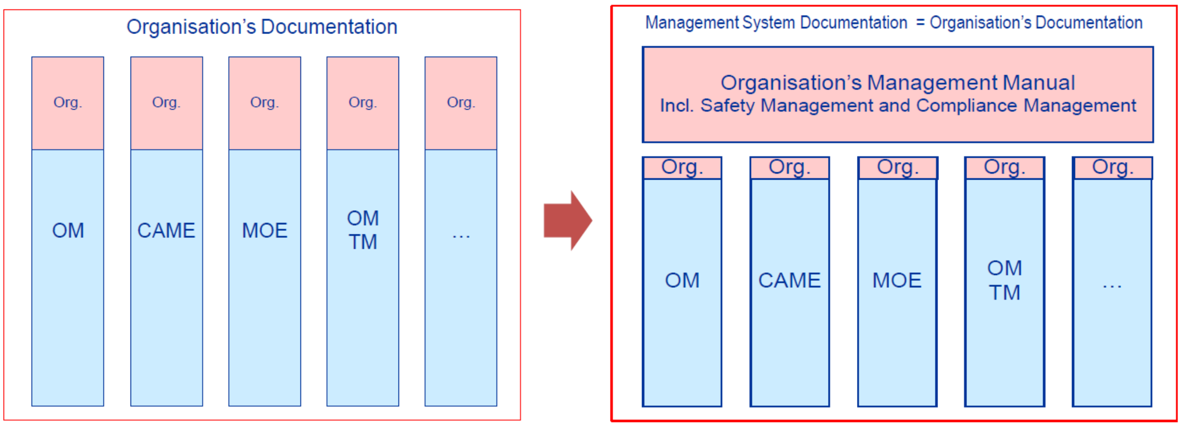

Organisation’s Documentation
Org.
Org.
Org.
Org.
Org.
OM
CAME
MOE
OM
TM
…
Management System Documentation = Organisation’s Documentation
Organisation’s Management Manual
Incl. Safety Management and Compliance Management
Org.
Org.
Org.
Org.
Org.
OM
CAME
MOE
OM
TM
…

Figure 4: Manuals for Integrated Management Systems, source: EASA

Even the Austrian SSP has no references to Part-IS, as it was last issued 2017, the text might give an idea, how to integrate an ISMS-Manual.

4.43 IS.OR.255 (a) Changes to the information security management system

Requirement

(a) Changes to the ISMS may be managed and notified to the competent authority in a procedure developed by the organisation. This procedure shall be approved by the competent authority.

ISO/IEC 27001 mapping

6.3 Planning of changes

A5.5 Contact with authorities

Part-IS particularity

Change Management is an inherent part of the ISMS under 6.3 of ISO/IEC 27001, but there is no provision for approval of a procedure by a competent authority.

In addition, most domain-specific implementing regulations mentioned in the "authority requirements" (namely ARO.GEN.310 (c), ARA.GEN.330 (c), CAMO.B.310 (h), 145.A.85 (c), ATM/ANS.AR.C.025 (c), ATCO.OR.B.015 (e), ADR.AR.C.035 (h)) of Reg. (EU) 2018/1139 allow a similar procedure for their changes.

Guidance for Part-IS implementation

It is recommended to use the same procedure, which is implemented for the "safety regulations" (see above) also for the approval of changes not requiring prior approval by the competent authority. This procedure should be extended to Part-IS in agreement with the competent authority.

Note:
This recommendation will only work, if the competent authority is the authority as laid down in Article 6 (1) of Reg. (EU) 2023/203 or Article 5 (1) of Reg. (EU) 2022/1645.

WARNING:
An organisation with a derogation approval according IS.OR.200 (e) needs to assess for all changes (also those not requiring prior approval) if the criteria for the approved derogation are still valid. If not, the change needs the approval of the competent authority/authorities prior to implementation of the change.

4.44 IS.OR.255 (b) Changes to the information security management system

Requirement

(b) With regard to changes to the ISMS not covered by the procedure referred to in point (a), the organisation shall apply for and obtain an approval issued by the competent authority.
With regard to those changes:

(1) the 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;

(2) the organisation shall make available to the competent authority any information it requests to evaluate the change;

(3) the change shall be implemented only upon receipt of a formal approval by the competent authority;

(4) the organisation shall operate under the conditions prescribed by the competent authority during the implementation of such changes.

ISO/IEC 27001 mapping

6.3 Planning of changes

A5.5 Contact with authorities

Part-IS particularity

Change Management is an inherent part of the ISMS under 6.3 of ISO/IEC 27001. However, ISO/IEC 27001 does not require any kind of approval by a competent authority.

In addition, all domain-specific implementing regulations (namely ORO.GEN.130, CAMO.A.130, 145.A.85, 21.A.147, 21.A.247, ATM/ANS.OR.A.040, ATCO.OR.B.015, ADR.OR.B.040, and UAS.LUC.070) of Reg. (EU) 2018/1139 require a similar procedure for their changes.

Guidance for Part-IS implementation

It is recommended to use the same procedure, which is implemented for the “safety-regulations” (see above) also for the approval, of changes in negotiation with the competent authority.

Note:
This recommendation will only work, if the competent authority is the authority as laid down in Article 6 (1) of Reg. (EU) 2023/203 or Article 5 (1) of Reg. (EU) 2022/1645.

4.45 IS.OR.260 (a) Continuous improvement

Requirement

(a) The organisation shall assess, using adequate performance indicators, the effectiveness and maturity of the ISMS. That assessment shall be carried out on a calendar basis predefined by the organisation or following an information security incident.

ISO/IEC 27001 mapping

9.3 Management review

10.1 Continual improvement

A5.35 Independent review of information security

Part-IS particularity

This requirement reflects a combination of the requirements 9.3 and 10.1 of ISO/IEC 27001 with reference to 4.4 and 5.2. While ISO/IEC 27001 focuses on ISMS suitability, adequacy, and effectiveness, Part-IS.OR.260(a) requires that the ISMS maturity be also periodically assessed.

Guidance for Part-IS implementation

ISO/IEC 27001 4.4 shows a clear requirement "shall" for ISMS maintenance and improvement. The top management has a responsibility for continual ISMS improvementimprovement as per ISO/IEC 27001 5.2(d). The planning section also requires continual improvement (ISO/IEC 27001 6.1.1(c).

OR.260 (a) requires an assessment of effectiveness and maturity of the ISMS on a calendar basis or following an information security incident. This assessment should be performed by using indicators. ISO/IEC 27001 chapter 9.3.1 defines a verysimilar approach for the management review process. chapter 10.1 indicates a more independent process to improve the ISMS. The process in Chapter 10.1 and is seen as more of a bottom-up approach, whereaswhile that in Chapter 9.3 is intended to be top-down.

The results from A5.35 should all be used as inputs for continuous improvement.

IS.OR.260 (a) requires also a maturity assessment of the ISMS.

Each organization should establish which maturity model will be followed and which targeted maturity level are expected to be reached and when.

For maturity assessment, AMC1 IS.I.OR.260 (a) chapter b) and GM1 IS.I.OR.260 (a) will provide guidance on how to ensure compliance to IS.OR.260 (a).

4.46 IS.OR.260 (b) Continuous improvement

Requirement

(b) If deficiencies are found following the assessment carried out in accordance with point (a), 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.

ISO/IEC 27001 mapping

10.2 Non-conformity and corrective action

A5.7 Threat intelligence

Part-IS particularity

IS.D.OR.260(b) addresses the improvement measures, i.e. corrections and corrective actions, for the deficiencies detected in IS.OR.260(a) and the continuous improvement process

This requirement reflects mainly to the requirements 10.2 of ISO/IEC 27001, even if the term used is “non-conformity, while IS.OR.260(b) uses the term “deficiencies”. Deficiency has a broader meaning than non-conformity. It encompasses the case of a targeted maturity level that would not be reached at the planned date, that would be a deficiency but not necessarily a non-conformity.

Guidance for Part-IS implementation

The provisions listed in ISO/IEC 27001 10.2 can be used to take corrective actions, to resolve both nonconformities and maturity level gaps.

AMC1 IS.OR.260(b) and GM1 IS.OR.260(b) will provide guidance on the process of decision making, implementation, and verification of the corrective actions.