Part-IS Implementation Task Force

Guidelines

Part-IS proportional implementation

Guidelines for Competent Authorities for the conduct of oversight activities on organisations that can be considered to be simple from a Part-IS[1] perspective

Part-IS TF G-04

June 2026

"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."

[1]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

Part-IS proportional implementation

Document ref.	Status	Date
Part-IS TF G-04	Issued	08/06/2026
Contact name and address for enquiries:	cybersec@easa.europa.eu European Aviation Safety Agency [Department] 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 provide 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	-
Authorised	N/A	Adopted by Part-IS Task Force	08/06/2026

Table of Contents

1 Executive summary 4

2 Introduction 5

3 Elements to be assessed by the competent authority and key considerations for the approval/oversight of simple organisations 6

3.1 Key considerations related to “Organisational structure” 12

3.2 Key considerations related to “Information Security Policy and Objectives” 15

3.3 Key considerations related to “Contracted Information Security management activities” (ref. IS.I/D.OR.235) 16

3.4 Key considerations related to the “Scope of the ISMS” 17

3.5 Key considerations related to “Risk management” 17

3.6 Key considerations related to “Incident management” 19

3.7 Key considerations related to “Internal and External reporting” 19

3.8 Key considerations related to “Record keeping” 19

3.9 Key considerations related to “Monitoring of compliance with Part-IS requirements” 20

Appendix 1: ISMS Scope and Risk Register 21

Appendix 2: Information Security Reports (related to the Internal Reporting Scheme) 24

1 Executive summary

This guidance provides a structured framework for competent authorities for the conduct of oversight activities on organisations that can be considered to be simple from a Part-IS perspective. Developed by the Part-IS Implementation Task Force under the European Union Aviation Safety Agency (EASA), these guidelines aim to standardise oversight activities and ensure compliance with *Commission Delegated Regulation (EU) 2022/1645* and *Commission Implementing Regulation (EU) 2023/203*.

2 Introduction

The introduction of information security management systems (ISMS) across the aviation industry brings some specific challenges for simple organisations and for authorities responsible for their approval and oversight. Although regulatory requirements are mandatory for organisations and competent authorities within the scope of the Regulation, their implementation should be proportionate to the nature and safety risk of the activities concerned, while also supporting the effective control of implementation and compliance costs.

This guidance has been written for any competent authority responsible for the approval and oversight of organisations that operate or provide services in civil aviation and which may be considered to be simple from a Part-IS perspective. It can be also used as guidance for those organisations since it contains elements on what would be expected by their competent authorities.

It must be noted that certain provisions of this document have some degree of deviation compared to the guidance provided in the document *"Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS"* also developed by the "Part-IS Implementation Task Force". The reason is that these provisions have been adapted to the particular case of organisations which are considered simple from the Part-IS perspective.

Coming to the question of when an organisation can be considered simple from the Part-IS perspective, it must be noted that size is not the only factor.

So, even when from other perspectives (e.g. SMS) it could be reasonable to talk about *Small* or *Very Small organisations,* this does not necessarily mean that these organisations can be considered "Simple" from an information security perspective.

In this case, the classification of simple or complex is based on three independent factors, in line with *Appendix V — "Proportionality considerations related to safety relevance and aspects of complexity" for AMC & GM to Part-IS.D.OR and Part_IS.I.OR (ED Decision 2025/014/R):*

- **Indicator of the degree of safety relevance: related to the organisation's role in the functional chain, and the number and criticality of interfacing organisations**

  The organisation's role in the functional chain (i.e. the line created by several organisations which are operationally connected) and its overall contribution to the safety of related functional processes are key indicators of safety relevance. This impacts the depth of risk assessment required and the level of assurance needed to ensure the effectiveness of measures implemented to mitigate unacceptable safety risks.

  NOTE: It must be noted that this indicator of degree of safety relevance includes also elements such as the category and/or number of aircraft operated by the organisation or using specific aerodromes, the type of products designed and/or produced, the systems/equipment used by ATM/ANS providers, etc.

- **Indicator of complexity 1: related to the complexity of the organisational structure and hierarchies**

  The complexity of an organisation's structure — typically determined by the number of staff, departments and hierarchical layers — directly influences the level of internal coordination

required and the extent to which information exchange needs to be formalised and proceduralised.

- **Indicator of complexity 2: related to the complexity of the Information and Communication Technology (ICT) systems and data used by the organisation.**

  The complexity of the information and communication technology systems and data used by the organisation, and their connection to external parties, directly influences the level of customisation and tailoring required for risk management and incident detection, response and recovery.

As a consequence, it is important for organisations to agree in each particular case with their competent authority what is the level of complexity/simplicity for each one of those factors, and to what level the organisation can be considered simple from the Part-IS perspective.

3 Elements to be assessed by the competent authority and key considerations for the approval/oversight of simple organisations

The following table contains the different elements that need to be assessed by the competent authority for the ISMS "Present" and "Suitable" levels (including readiness to start operating the ISMS) during the initial implementation of Part-IS. It is an adaptation for simple organisations of the table contained in the *"Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS"* issued by the "Part-IS Implementation Task Force".

NOTE: Further material will developed at a later stage for the assessment of the "Operating" and "Effective" levels.

In addition, for some elements, key considerations and examples have been provided in order to help the competent authority to achieve a proportional approach during the approval/oversight of simple organisations.

As a general consideration related to **organisations characterised by a combination of limited number of staff members, few hierarchical layers and few departments**, it is acceptable that the organisation provides simplified policies and procedures. In particular:

- **Streamlined documentation:** Policies and procedures can be concise, clear and easy to read., with documents being kept short and simple to make them easily understandable. Templates may be used in order to expedite the creation of the necessary documentation but should be tailored to match the organisation.
- **Focus on key policies:** During the initial implementation, the key policies may be prioritised in order to address the most critical aspects of information security, such as management commitment, access control and incident response.

Furthermore, it may be useful for these organisations to integrate these simplified processes and procedures within those already used for SMS implementation.

Table 1: Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS) for simple organisations

NOTE: In line with the *"Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS"* issued by the "Part-IS Implementation Task Force", the review of the elements contained in the "ISMM review" column in the table below (which may include not only a desktop review of the ISMM, but also discussions and clarifications with the organisation) is required for the initial approval of the ISMM, while the audit of the elements contained in the "Audit" column may be done later by integrating it into the on-going oversight activities of the organisation. This audit may combine elements audited onsite and elements audited remotely and may also take the form of assessments and inspections.

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I.OR.240 Organisational structure **NOTE: Refer to Item 3.1 after this table for key considerations related to "Organisational structure"**	a) Has the structure been updated to reflect the ISMS (e.g. appointment of an information security manager, reporting structure)?	•	
	○ Have their functions and responsibilities been defined ○ Is there a link between safety, security and information security functions?	•	•
	Where the organisation has decided to appoint a CRP (Common Responsible Person), does the person have sufficient capacity and delegated authority to effectively implement Part IS in the organisation?	•	•
	b) Has the organisation developed a framework/policy to address the different levels of trustworthiness of the workforce? Have the current staff been already assessed for trustworthiness?	•	•
	c) Has the organisation developed a competence framework and evaluation process? Have the current staff been already assessed for competence?	•	•

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I.OR.200(a)(1) Information security policy and objectives **NOTE: Refer to Item 3.2 after this table for key considerations related to "Information Security Policy and Objectives"**	a) Has the organisation developed a clearly defined information security policy?	•	
	○ Is the purpose of the policy clearly stated?	•	
	○ Are the information security objectives defined?	•	
	○ Is the concept of aviation safety an integral part of the policy?	•	
	○ Is the content of the policy appropriate to the complexity of the organisation?	•	•
	○ Is there a reference to the organisation's information classification scheme?	•	
	b) Is the policy available to all staff/contracted parties and has been properly communicated?		•
	c) Have criteria been established for the review of the policy?	•	•
IS.I.OR.255 Change management	a) Has a procedure for change management been developed by the organisation and has the organisation applied for approval to the appropriate authorit(y/ies)?	•	
IS.I.OR.235 Contracted Information Security management activities	a) Has the organisation defined which IS management activities are contracted, if any, to third parties (Ref. IS.D/I.OR.235) and the appropriate contracts have been established?	•	•
	b) Are there procedures defining how the organisation is performing oversight of IS management contracted activities and managing any associated risk?	•	

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
NOTE: Refer to Item 3.3 after this table for key considerations related to "Contracted Information Security management activities"	c) Has the organisation ensured appropriate access of the Competent Authority to the contracted parties and included this in the corresponding contracts?	•	•
IS.I.OR.205(a) and (b) Scope of the ISMS **NOTE: Refer to Item 3.4 after this table for key considerations related to "Scope of the ISMS"**	a) Has the scope (e.g. services, systems, assets, processes, interfaces and perimeter) of the ISMS been defined with proper justifications of the outcome and any exclusions?	•	•
IS.I.OR.205 and 210 Risk management **NOTE: Refer to Item 3.5 after this table for key considerations related to "Risk management"**	a) Has a formal process for information security risk management been established?	•	•
	○ Are there the three main processes or procedures (i.e. Risk identification, Risk assessment and Risk treatment) defined within the risk management context?	•	
	○ Are risk acceptability criteria and responsibilities clearly defined?	•	
	b) Has the organisation defined how the risks related to operational contractors/suppliers will be managed (this does not include contracted Information Security management activities covered by points IS.I.OR.235 and IS.D.OR.235, which are addressed further below in this table)?	•	•
	c) Has the organisation performed an initial risk assessment (e.g. major risks and related threat scenarios both internal and at the interfaces)?	•	•
	d) Does the organisation have provisions for an asset inventory (processes, software, hardware) (e.g. template described in the ISMM) ?	•	

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
	e) Has the organisation already included the applicable assets in the inventory?		•
IS.I.OR.220 Incident management (Detect, Respond, Recover) **NOTE: Refer to Item 3.6 after this table for key considerations related to "Incident management"**	a) Are there procedures in place to detect information security incidents, including monitoring mechanisms for potential threats?	•	
	b) Are there procedures in place to respond to detected incidents in a timely manner (e.g., initial containment measures)?	•	
	c) Are there procedures in place to recover from incidents and to return to proper safety level after an incident?	•	
	d) Are the implemented measures adequate and suitable to respond to and recover from information security incidents?		•
IS.I.OR.215 and 230 Internal and External Reporting **NOTE: Refer to Item 3.7 after this table for key considerations related to "Internal and External reporting"**	a) Are there procedures for reporting of events within the organisation and from external parties? Are the staff and external parties informed about such procedures?	•	•
	b) Are there procedures and responsibilities defined for evaluation of events and decision of which ones have to be considered incidents or vulnerabilities?	•	
	c) Has the organisation developed a procedure to identify which incidents and vulnerabilities have to be reported through the external reporting system?	•	
	d) Have procedures for external reporting been defined (including all the stages of reporting, root cause analysis, follow up etc.)?	•	
	e) Are the staff involved in the processing of internal and external reports properly identified, trained and authorized?		•
IS.I.OR.245 Record keeping	a) Are there procedures defining which records are retained, the retention period and the format of those records?	•	

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
NOTE: Refer to Item 3.8 after this table for key considerations related to "Record keeping"	b) Has the organisation defined the appropriate records protection (e.g. against damage, alteration, theft, unauthorised access etc.	•	•
IS.I.OR.200(a)(6) and (a)(7) Measures and findings notified by the competent authority	a) Has the organisation defined procedures to implement measures notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety?	•	
	b) Has the organisation defined procedures to address findings notified by the competent authority?	•	
IS.I.OR.200(a)(13) Protection of the confidentiality of information received from other org's	a) Has the organisation defined procedures to protect the confidentiality of information received from other organisations, according to its level of sensitivity?	•	
IS.I.OR.200(a)(12) Monitoring of compliance with Part-IS requirements **NOTE: Refer to Item 3.9 after this table for key considerations related to "Monitoring of compliance with Part-IS requirements"**	a) Has the organisation made available an internal compliance monitoring report, describing the organisational level of compliance with all the criteria described in the columns "ISMM" and "Audit" of this table?	•	

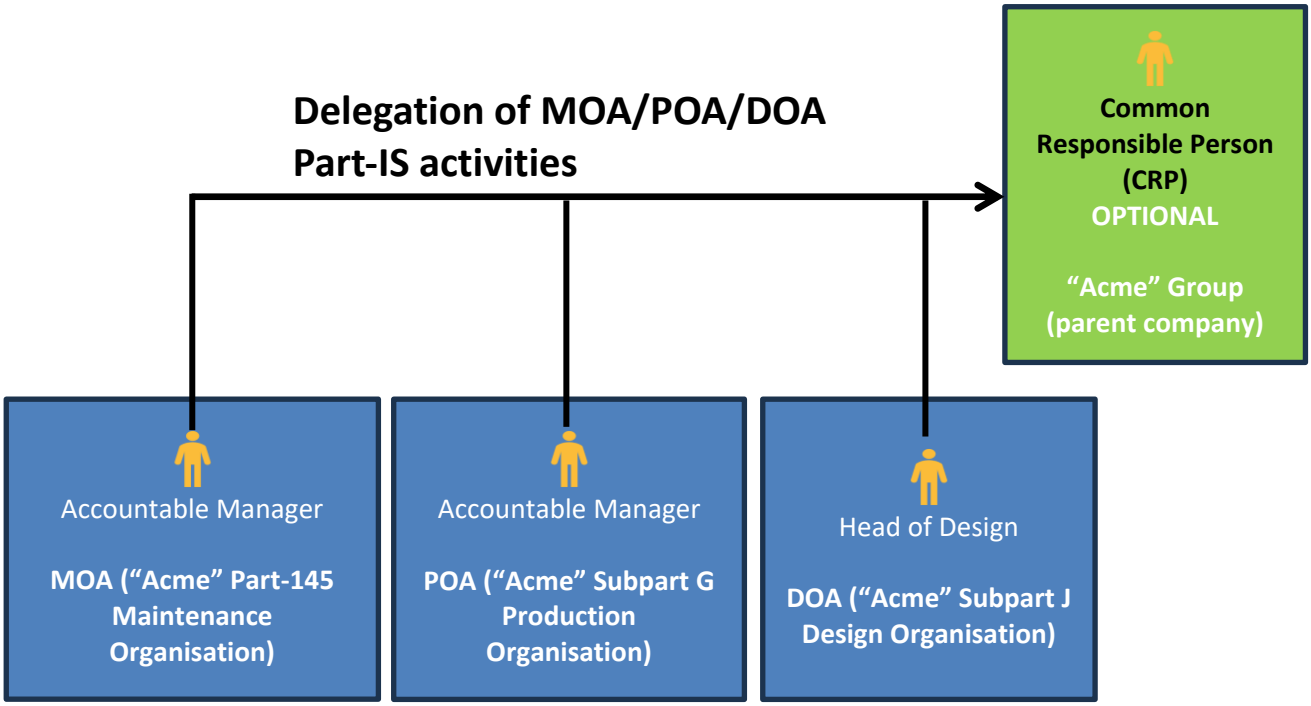
3.1 Key considerations related to "Organisational structure"

Regarding the organisational structure of a simple organisation, different arrangements and combinations of positions may be acceptable if the proper responsibilities can be discharged and the corresponding persons have the appropriate competences.

In addition, it must be noted that some simple organisations may hold several approvals (e.g. DOA/POA/MOA) and may share information security organisational structures, policies, processes and procedures across those approvals. In such case, IS.I/D.OR.240(d) allows (OPTIONAL) the accountable manager (or Head of Design) of each approval to delegate its activities to a Common Responsible Person (CRP), as long as coordination measures have been established between each Accountable Manager/Head of Design and the Common Responsible Person to ensure adequate integration of the information security management within each organisation.

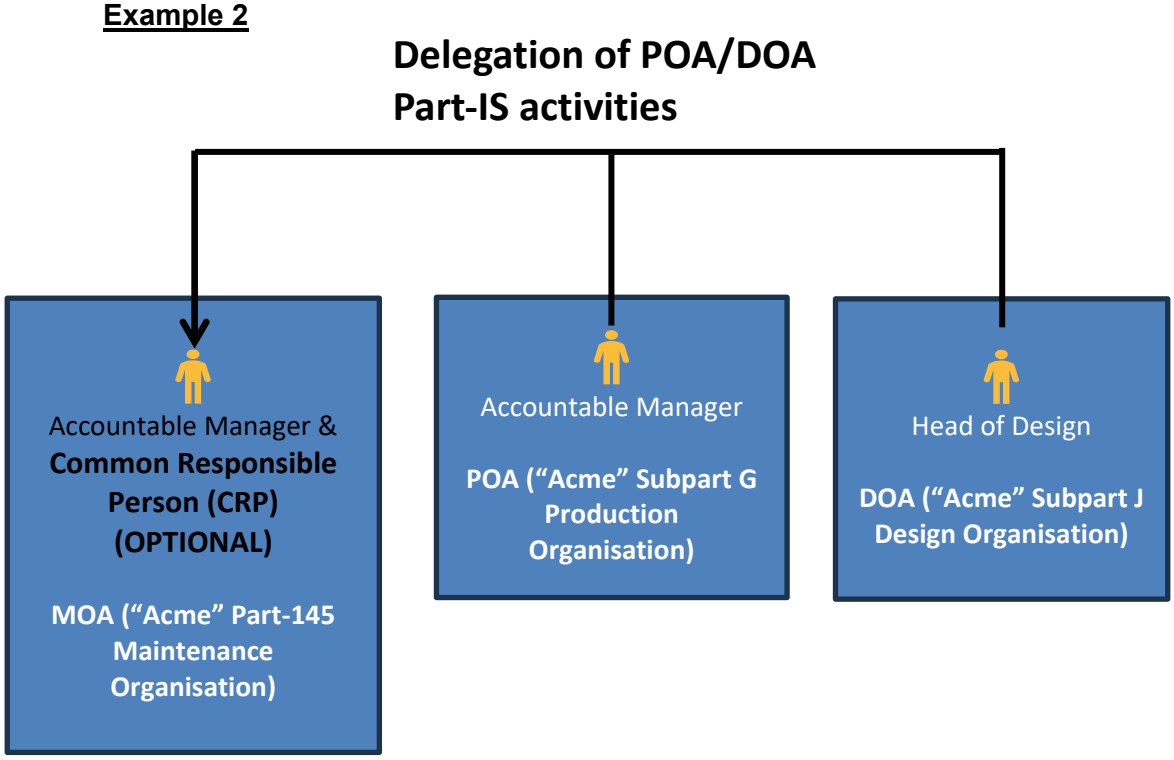
This Common Responsible Person may be one of the existing Accountable Manager(s)/Head of Design, or may be a separate person at corporate level, as reflected in the two examples below:

Example 1



NOTE: As indicated in the example above, the Common Responsible Person (CRP) may be hierarchically above the Accountable Managers/Head of Design. This would be the case where the CRP is not part of the staff of the MOA/POA/DOA but holds a high management position in the Corporate Organisation (e.g. Parent Company) owning the MOA/POA/DOA.

Example 2



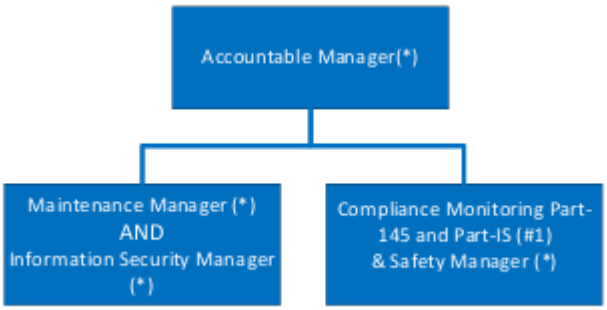
In the particular case, for example, of a simple Part-145 maintenance organisation, some examples (non exhaustive) of arrangements that may be acceptable are the following:

NOTES:

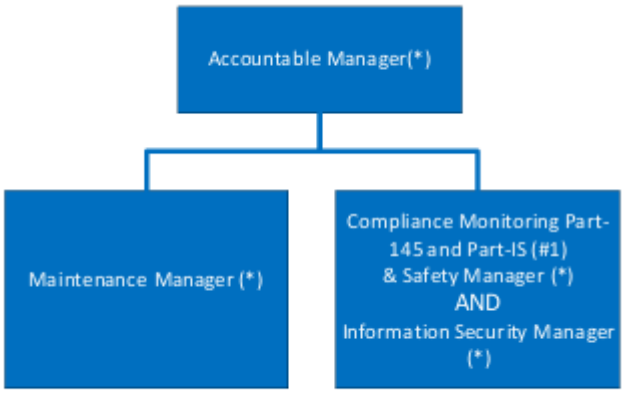
- *The symbol (*) in the examples below means "Nominated/Appointed Person"*
- *The symbol (#1) in the examples below mean that, regarding the nominated person(s) for Compliance Monitoring, the organisation may nominate two separate persons for the positions of "Compliance Monitoring Manager Part-145" and "Compliance Monitoring Manager Part-IS" or may nominate the same person for both positions.*

Example 3

Example 4



Example 5



NOTE: This combination of positions may only be accepted if the organisation ensures the independence of the internal audit of the compliance monitoring function (incl. information security aspects of ISMS) by having the annual internal audit conducted by an independent auditor.

Regarding the competence of staff, the following approach should be considered acceptable when assessing organisations characterised by a combination of limited number of staff members, few hierarchical layers and few departments:

- **Targeted Training Programs**: Focused training programmes that target the specific roles and responsibilities of employees are provided, with the training being relevant to the organisation's specific risks and operational context.

- **Security Awareness:** Short training sessions and/or awareness campaigns are conducted on a regular basis in order to encourage adequate awareness of information security threats throughout the organisation.

3.2 Key considerations related to "Information Security Policy and Objectives"

The competent authority should place particular attention in verifying that the Information Security Policy is specifically adapted to each particular organisation. For this purpose, it may be useful that the organisation integrates this Information Security Policy within the Safety Policy already established during SMS implementation.

Furthermore, the competent authority should check that the Information Security Policy includes appropriate consideration of the interactions between information security risk management and aviation safety risk management.

Regarding the information security objectives established by the organisation in order to meet the Information Security Policy, the competent authority should check that those objectives are always relevant to the improvement of aviation safety.

Regarding Key Performance Indicators (KPIs), they should be SMART (specific, measurable, attainable, realistic and timely) in order to properly measure how the objectives are met. Some examples are the following:

- Regarding "Risk Assessment and Treatment":
  - Ratio of information security Threats identified for the existing safety hazards.
  - Number of information security assessments during assessment of new/changed hazards
- Regarding "Policies and Procedures":
  - Number of "Part-IS related" non-compliance issues identified during internal/external audits.
- Regarding "Security Controls (measures)":
  - Ratio of performed vs. planned security control validations (e. g. Log-Review, Access-Control validation).
- Regarding "Incident Management":
  - Trend of incidents (resulting from information security events) with impact on safety over time (e.g. annual trend monitoring).
- Regarding "Training and Awareness":
  - Training completion rate: % of employees completing information security (awareness) training.

When using indicators, it is also important to consider proportionality, not being expected that simple organisations define a large number of KPIs, but just the few most relevant ones. Furthermore, when measuring quantities, for example, a number too low may indicate a lack of ISMS effectiveness, while a number too high may sometimes suggest that the matter is becoming an end in itself, which is not necessarily appropriate for a properly functioning ISMS.

3.3 Key considerations related to "Contracted Information Security management activities" (ref. IS.I/D.OR.235)

Organisations may decide to outsource certain activities to suppliers. This covers both operational activities (i.e. core activities required by each domain-specific regulation and not linked to Part-IS requirements), as well as information security management activities required by Part-IS.

- In the case of contracted operational activities (i.e. core activities required by each domain-specific regulation and not linked to Part-IS requirements), the related information security risks need to be managed in accordance with points IS.I/D.OR.205 and IS.I/D.OR.210.
- On the other hand, in the case of contracted information security management activities, the related information security risks need to be managed in accordance with IS.I/D.OR.235.

Despite those differences, it may be useful for simple organisations to integrate and use similar processes for both cases, addressing the information security risks of their supply chain as a whole package.

In addition, it must be noted that when contracting certain activities to third parties (contracted organisations), the contracting organisation remains responsible for the oversight of the contracted organisation(s) and accountable for compliance with the applicable requirements.

Although the possibility of outsourcing and the possibility of collaboration with peers from other organisations or industry groups is open to any organisation, the approach described below may be specially useful for organisations characterised by a combination of limited number of staff members, few hierarchical layers and few departments:

- **Outsourcing**: For areas where the organisation lacks expertise, outsourcing to providers of managed-security services may be adopted.
- **Collaboration with Peers:** Information-sharing may be established with similar organisations or industry groups (e.g. the European Centre for Cyber Security in Aviation (ECCSA)). This type of collaboration provides insights to evaluate the evolution of the security environment with a more limited effort.

Examples of information security management activities that may be contracted are provided in GM3 IS.I/D.OR.235.

3.4 Key considerations related to the "Scope of the ISMS"

The competent authority should focus their attention on evaluating whether the organisation has properly defined the following:

- the organisation's activities, facilities and resources, as well as the services that the organisation operates, provides, receives or maintains.
- the equipment, systems, data and information that contribute to the functioning of the elements listed above.
- The interfaces that the organisation has with other organisations, and which could result in the mutual exposure to information security risks.

and whether the organisation has conducted an impact analysis to include or exclude the above items based on their safety relevance.

For simple organisations, it may be useful to start with the list of risks identified within the SMS framework and evaluate which ones could be caused by information security threats, identifying the associated elements/assets (e.g. activities, facilities, resources, services, equipment, systems, data and information) and interfaces affected.

In the particular case, for example, of a Part-145 maintenance organisation, typical examples (not exhaustive) of interfaces with other organisations, which may result in the mutual exposure to information security risks that could be safety-relevant are the following:

- Interface with CAMOs who provide Work Orders, Instructions for Continued Airworthiness (ICAs), information on aircraft configuration, list of deferred items, MEL information, etc.
- Interface with OEMs and DOAs who provide access to Instructions for Continued Airworthiness (ICAs), repair instructions, software for the update of avionic systems, etc.
- Interface with suppliers of parts, tools, test equipment (including, for example, software update for test equipment), etc.
- Interface with contractors and subcontractors (for specialised tasks, maintenance activities, etc), also possibly including maintenance teams of the manufacturer.
- Interface with training organisations for maintenance personnel.
- Interface with the competent authority.

3.5 Key considerations related to "Risk management"

For simple organisations it may be useful to use similar risk assessment methodologies for SMS and ISMS in order to enable a close link between information security and aviation safety.

When assessing organisations whose role in the functional chain and its interfaces do not pose a significant risk of unsafe conditions, the following approach should be considered acceptable:

- **Simplified Risk Assessment**: A streamlined risk assessment process that prioritises risks based on their potential impact on safety may be used. The assessment may focus on the higher-impact areas, with more detailed assessments being performed only where and if necessary.
- **Risk Treatment Prioritisation**: A risk treatment plan that prioritises high-impact risks with cost-effective measures may be adopted. In such cases, cost-effective controls that reduce risks to acceptable levels may be used. These controls can often leverage existing processes, physical controls or technology.

Note: Refer to Appendix 1 for a typical example of ISMS Scope and Risk Register for a simple organisation, and for more details on criteria to use in defining the scope of the ISMS, evaluating likelihood and defining risk.

The following is a list of typical examples (not exhaustive) of information security risks that may be faced by a Part-145 maintenance organisation. These information security risks may have an impact on safety (e.g. if they lead, for example, to the aircraft being maintained by personnel not properly qualified, or to a potential unairworthy state), which needs to be evaluated during the safety risk assessment:

- The Maintenance Management Software used by the organisation being compromised (regardless of whether it is their own software or access is provided through the CAMO).
- Unauthorised use of electronic signatures (e.g. maintenance release documents issued by unauthorised persons or simulating an authorised person). NOTE: To a lower scale, this could also be a risk for paper releases.
- Use of compromised keys to encrypt and decrypt data transmitted between organisations.
- Use of compromised Instructions for Continued Airworthiness (ICAs).
- Use of compromised Work Orders.
- Aircraft/engine upload of compromised software (e.g. navigation data) or downloaded of software from unreliable sources or using faulty hardware to store the data.
- Use of compromised qualification records (e.g. training, experience, phycological evaluations…), either digital or paper based, resulting in unproper certifying staff authorisations.
- Reliance on compromised tool/equipment calibration records.
- Reliance on compromised information in the Approved Capability List, resulting in the performance of non-authorised maintenance.

NOTE: Regarding the use of an electronic signature system for releasing maintenance on an EASA Form 1, guidance can be found in “AMC to Appendix II to Part-M – Use of the EASA Form 1 for maintenance” (ref. pages 132-134 of ED Decision 2015/029/R).

3.6 Key considerations related to “Incident management”

When assessing organisations characterised by a combination of usage of a few Information and Communication Technology (ICT) tools and utilisation of standard ICT products, the following approaches should be considered acceptable:

- **Simplified Incident Management:** A basic incident management process that allows for quick identification, reporting and response to security incidents may be adopted, with lessons learned from incidents being integrated into the ISMS for continuous improvement.
- **Automated Tools**: Automated tools for monitoring, logging, and managing security incidents may be used in order to reduce manual effort while maintaining continuous compliance.

For example, a simplified incident management approach may consist on the establishment of a predefined list of events (e.g. when an application starts not responding, a when a suspicious message is received, etc), known by the workforce, that trigger the reporting process and the activation of the incident management function. A set of standardised response actions is defined in advance for each type of event and documented in concise documents (e.g. 'playbooks'), enabling consistent and timely reaction by staff.

3.7 Key considerations related to “Internal and External reporting”

In the case of Internal Reporting, it may be useful for simple organisations to integrate this process within the one they already have for SMS internal reporting, while taking into account, if that is the case, the peculiarities introduced by any contracting out of the handling of information security incidents.

In the case of External Reporting, it is expected that the organisation uses the existing process that they have already implemented for external safety reporting via ECCAIRS2. It must be noted that ECCAIRS 2 has been updated to include also a taxonomy relevant to information security incidents (including vulnerabilities).

3.8 Key considerations related to “Record keeping”

When assessing organisations characterised by a combination of usage of a few Information and Communication Technology (ICT) tools and utilisation of standard ICT products, the following approaches should be considered acceptable:

- **Essential Records**: Only records that are essential to demonstrate compliance and the effectiveness of the ISMS are kept. Excessive documentation that does not add value or is burdensome to maintain is avoided.

- **Use of Digital Solutions:** Digital tools are used for document management to simplify access and version control, and to ensure the security of records.

3.9 Key considerations related to "Monitoring of compliance with Part-IS requirements"

Although this is possible for any organisation, it may be specially useful for simple organisations to integrate the compliance monitoring of Part-IS requirements within the compliance monitoring process already existing in the organisation as part of the SMS implementation. This may include using the same person(s) to audit compliance with both SMS and ISMS requirements. In such a case, the competent authority should pay particular attention to ascertain that the auditors have the proper qualifications to audit both domains.

When assessing organisations characterised by a combination of limited number of staff members, few hierarchical layers and few departments, the following approach should be considered acceptable regarding Internal Compliance Monitoring and Continuous Improvement:

- **Regular but Scaled Audits**: Internal audits are regularly conducted, but the effort is scaled to the organisation's size and complexity. The focus is on the most critical areas, while less critical areas could be audited on a less frequent basis. Audit results are provided to the accountable manager or the head of the design organisation and utilised to guide continuous improvement.

  It must be noted that in the case where the organisation has the management structure described in Example 5 of item 3.1, the organisation needs to ensure the independence of the internal audit of the compliance monitoring function (incl. information security aspects of ISMS) by having the annual internal audit conducted by an independent auditor.
- **Agile Review Process**: The ISMS is regularly reviewed and, if necessary, adapted to ensure that it remains aligned with the organisation's evolving needs and threats.

Appendix 1: ISMS Scope and Risk Register

A typical example of ISMS Scope and Risk Register for a simple organisation may look as follows:

Scoping

The scope of the ISMS is defined by the list of safety-relevant processes that could be impacted by information security threats, along with the associated information systems and interfaces with other organisations. The following information is therefore expected:

- Process name.
- Short description of the process.
- High-level, safety-relevant events that would be expected if the information or data used throughout the process lose either their integrity, availability or confidentiality.
- Formalisation of the safety consequence. Here different approaches can be used (ICAO impact scales, the proposed approach in ER-040).
- Description of the information systems that are used for the information and data processing in the safety relevant processes.

Likelihood evaluation

To identify the risks starting from the above list of elements in scope, a likelihood evaluation is needed. Likelihood answers one question: How realistic is it that the threat and the related safety-relevant event could actually happen in our organisation?

To answer this, the organisation should at least assess the following aspects:

- Window of opportunity / Exposure of vulnerability
- Difficulty to Prepare the Attack
- Difficulty to Perform the Attack

A structured approach, albeit simple, would help to avoid typical biases that affect likelihood evaluations. For example, scoring low based on the idea that 'this has never happened before', or assuming that attackers must be highly technical should be avoided. Similarly, personal confidence can lead to over- or underestimation. Reflecting on the above aspects needs to focus on realistic opportunity and effort rather than theory.

Example

Each aspect can be scored e.g. from **1 (Low) to 3 (High).**

1. Window of Opportunity / Exposure of vulnerability

Question: *How easy is it for someone to find the right moment to try this?*

Score	Guidance
1 – Limited	Only during rare or exceptional situations
2 – Occasional	Possible at certain times or conditions
3 – Frequent	Possible during normal, day-to-day operations

Note: If it could happen **on a normal working day**, choose **3.**

2. Means & Knowledge to Prepare the Attack

Question: *How hard is it to get ready for this attack?*

(Think about skills, tools, time, and access needed before the attack in order to know how the systems work and where they have any vulnerabilities.)

Score	Guidance
1 – Difficult	Requires specialist skills or insider knowledge is needed to know how your systems work.
2 – Moderate	Guides/tools exist but require effort to understand, and the information about how your systems work is reasonably protected.
3 – Easy	Ready-to-use tools or tutorials are widely available, and the information about how your systems work is easily accessible (e.g. public information)

Note: If a **motivated non-expert** could learn all this, choose **2 or 3**.

3. Means & Technical Capability to Perform the Attack

Question: *Once ready, how difficult is it to carry it out and reach a safety consequence?*

(Think about controls, monitoring, approvals, and human factors. Also factor in any existing controls that may have been introduced to mitigate traditional safety risks.)

Score	Guidance
1 – Hard	Strong controls likely stop the attempt
2 – Some barriers	Controls exist but may be bypassed
3 – Very easy	Few controls and reliance on non-verified trust

Note: If the first attempt would **likely succeed**, choose **3.**

Calculating Likelihood

Add the three scores:

Likelihood Score = Opportunity + Preparation + Execution

Total	**Likelihood**
3–4	Low
5–6	Medium
7–9	High

Output to Record (Minimum)

For each threat scenario, record:

- The three scores
- A one-line justification per score
- The total likelihood level

Risk determination and recording

The risk assessment is determined by combining safety consequences and likelihood considerations. The following information is therefore expected:

- Description of how the risk is determined as a function of safety impact and likelihood (in most cases, we expect a so-called 'risk matrix') and which risks are proposed to be retained (risk acceptability boundary/area).
- Description of the mitigations and controls implemented or intended to be implemented (and possibly their effectiveness if already implemented).
- A risk register in the form of a summary table, listing risks by their unique IDs alongside essential information.

Appendix 2: Information Security Reports (related to the Internal Reporting Scheme)

NOTE: This Appendix is not applicable for those cases where the organisation has decided to integrate the Internal and External Reporting Schemes, since in that case the structure and process related to the ECCAIRS2 system is applicable.

A typical Information Security Internal Report for a simple organisation is expected to contain the following information:

- Part A to be completed by the person identifying the information security issue or hazard:
  - Date and time of event
  - Location of the event
  - Name of the reporter
  - Description of the event or identified hazard and suggestions to prevent similar occurrences.
  - Opinion of the reporter regarding:
    - Likelihood of such an event or similar happening or happening again (e.g. unlikely, probable, likely)
    - Worst possible consequence if this event did happen or happened again (e.g. negligeable, significant, etc)

- Part B to be completed by the person or committee responsible for evaluation the report:
  - Likelihood of the event occurring or recurring (e.g. unlikely, probable, likely…)
  - Degree of the most credible worst-case consequences (e.g. negligible, serious incident, fatal accident…)
  - What action or actions have been or are being taken to prevent the issue or hazard from occurring in the future and/or to mitigate its consequences.
  - Resources required.
  - Who is responsible for the action.

- Part C:
  - Signature/acceptance by responsible manager and corresponding nominated person.
  - Confirmation of feedback provided to the staff who initially reported.
  - Follow-up actions.