Part-IS Implementation Task Force

Guidelines

Part-IS oversight approach

Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS[1]

Part-IS TF G-03

March 2025

"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 oversight approach

Document ref.	Status	Date
Part-IS TF G-03	Issued	10/03/2025
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	10/03/2025

Table of Contents

1 Executive summary

This guidance provides a structured framework for competent authorities to oversee the implementation of Information Security Management Systems (ISMS) in aviation organizations. 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 Implementation of ISMS in Aviation: A Continuous Process of Growth & Maturity[2]

The establishment of a mature Information Security Management System (ISMS) within any aviation domain is a task which evolves over time. It is an ongoing process that requires continuous improvement, adaption and development. In addition, a key concept is that the Part-IS requirements have varying significance during the foundation and operational phases of the ISMS. Certain provisions are crucial for establishing the foundation of the ISMS. Once established, these provisions take a background role, while other requirements become more relevant during operations.

The below table shows the relevance of different requirements with respect to the foundation and operational stages.

Table 1: Requirements relevance in the ISMS Foundation and Operational stages

Part-IS requirement	Description	Relevance (High /Background)	
		ISMS Foundation	ISMS Operation
IS.I/D.OR.100	Scope definition	High	Background
IS.I/D.OR.200	Information security management system	High	Background
IS.I/D.OR.205	Information security risk assessment	High	Background
IS.I/D.OR.210	Information security risk treatment	High	Background
IS.I/D.OR.215	Information security internal reporting scheme	Background	High
IS.I/D.OR.220	Information security incidents — detection, response, and recovery	Background	High
IS.I/D.OR.225	Response to findings notified by the competent authority	Background	High
IS.I/D.OR.230	Information security external reporting scheme	Background	High
IS.I/D.OR.235	Contracting of information security management activities	Background	High
IS.I/D.OR.240	Personnel requirements	High	Background
IS.I/D.OR.245	Record-keeping	Background	High
IS.I/D.OR.250	Information security management manual	High	Background
IS.I/D.OR.255	Changes to the ISMS	High	Background
IS.I/D.OR.260	Continuous improvement	Background	High

In light of this, and for the purpose of standardising the oversight performed by the different competent authorities, the following **implementation levels** of the ISMS are considered: **"Present," "Suitable", "Operating,"** and **"Effective" (PSOE).**

[2] *In this document, reference to the particular requirements of Part-IS have been identified as IS.**I/D**.OR.XXX, where "I" makes reference to Implementing Regulation (EU) 2023/203, and "D" makes reference to Delegated Regulation (EU) 2022/1645. As such they should be read as meaning to include the references to IS.**I**.OR.XXX and IS.**D**.OR.XXX.*

"Present" and "Suitable" levels correspond to the "ISMS foundation" elements indicated in the table above.

"Operating" level corresponds to the "ISMS operation" elements indicated in the table above. This is the level that should be reached for the organisation to be considered as Part-IS compliant.

The "Effective" level corresponds to the subsequent "continuous improvement" that should be pursued by the organisation once compliance with the requirements has been achieved. In this regard, and for the purpose of complying with the "Continuous Improvement" requirements contained in points IS.I.OR.260 and IS.D.OR.260 of Part-IS, the concept of "maturity" is introduced. The organisation may use the different Maturity Models described in GM1 IS.I.OR.260(a) and GM1 IS.D.OR.260(a). It must be noted that no specific maturity level is required. However, if and when compliance ("operational" level) is achieved, organisations will determine which requirements of which models have already been met (mandatory) and can opt to reach a level that is beneficial to the organisation (voluntary). In the longer term, achieving higher maturity levels may increase the confidence of oversight authorities, which can have an impact upon the level of oversight activities regarding such organisation.

2.1 Responsibilities of Organisations and Authorities

Organisations should:

- **Implement an ISMS at the "Present and Suitable" level by the applicability date of the relevant Part-IS regulation** (i.e. 16 October 2025 for organisations covered by Delegated Rule (EU) 2022/1645, and 22 February 2026 for organisations covered by Implementing Regulation (EU) 2023/203, **and perform, by that date, a Compliance Monitoring activity to ensure that the organisation meets those requirements.**
- **Start operating such ISMS immediately after the applicability date.**

NOTE: Organisations intending to apply for a derogation in accordance with point IS.I.OR.200(e) or IS.D.OR.200(e) and authorities involved in the approval of such derogations may refer to the document "Implementation guidelines for Part-IS – IS.I/D.OR.200(e)" developed by the Part-IS Implementation task Force.

Competent authorities are responsible for assessing the implementation of ISMS. To that end, they may use the guidelines and timelines contained in this document, or guidelines and timelines developed at national level as prescribed by the relevant authority requirements (e.g. ARO.GEN.300(b)(1)). In that regard, and since ISMS implementation is a progressive process, the competent authority may follow a phased approach in accordance with point 2.2 below.

The organisation will be deemed to have reached Part-IS compliance once the authority has completed all the phases allowing it to conclude that the organisation has reached the "Present", "Suitable" and "Operating" implementation levels. This assessment process is not expected to be completed until well after the applicability date, since it is necessary for the ISMS to be operating and producing results during a reasonable and sufficient amount of time, the authority needs to perform the appropriate audits, assessments and inspections, and any findings need to be addressed.

2.1.1 Step 1: Assessment of ISMS implementation at "Present" and "Suitable" levels

At this stage, the goal is for the competent authority to assess whether the organisation has demonstrated that the foundation elements of the ISMS are established, and the organisation is in a position to operate the ISMS. Most of the evidence that the organisation should provide for the authority's assessment of a present and suitable implementation of the ISMS is expected to be part of the Information Security Management Manual (ISMM), whereas the remaining evidence may only be reviewed during an audit of the organisation. Typical elements that should be checked by the competent authority as part of the ISMM review, and typical elements to be checked during an audit of the organisation are contained in the table below.

It is important to note that the table below contains not only elements related to the availability of appropriate procedures and structures. It also contains elements aimed at verifying that the organisation has implemented those procedures at a sufficient level that allows them to operate the ISMS. Some examples are the following:

1. Staff have already been assessed for trustworthiness and competence (commensurate with their role and involvement in safety and/or information security critical activities).
2. The information security policy is available to all staff and contracted parties and has been properly communicated.
3. The scope (e.g. services, systems, assets, processes, interfaces and perimeter) of the ISMS has been defined with proper justifications of the outcome and any exclusions.
4. The organisation has performed an initial risk assessment (e.g. major risks and related threat scenarios both internal and at the interfaces).
5. Staff and external parties have been informed about the existing reporting procedures.
6. Staff involved in the processing of internal and external reports are properly identified, trained and authorized.
7. If the organisation has contracted information security management activities to third parties, the applicable contracts have been already established.

This assessment by the authority should take into account also the initial risk assessment and the evidence of compliance monitoring activities that the organisation needs to make available to the competent authority as described in Section 3, Step 1, below.

NOTE: As described in Section 3 below, the review of the ISMM elements (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 organisation 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.

Table 2: Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I/D.OR.240 Organisational structure	a) Has the structure been updated to reflect the ISMS (e.g. appointment of an information security manager, reporting structure)?	●	
	○ Is there a link between safety, security and information security functions?	●	●
	b) 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?	●	●
	c) 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?	●	●
	d) Has the organisation developed a competence framework and evaluation process? Have the current staff been already assessed for competence?	●	●
IS.I/D.OR.200(a)(1) Information security policy	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?	●	●

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
	○ 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/D.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/D.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?	•	
	c) Has the organisation ensured appropriate access of the Competent Authority to the contracted parties and included this in the corresponding contracts?	•	•
IS.I/D.OR.205(a) and (b) 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/D.OR.205 and 210 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	•	•

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
	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) ?	•	
	e) Has the organisation already included the applicable assets in the inventory?		•
	f) Has a formal process for information security risk management been established?		•
IS.I/D.OR.220 Incident management (Detect, Respond, Recover)	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/D.OR.215 and 230 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?	•	

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
	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/D.OR.245 Record keeping	a) Are there procedures defining which records are retained, the retention period and the format of those records?	•	
	b) Has the organisation defined the appropriate records protection (e.g. against damage, alteration, theft, unauthorised access etc.)	•	•
IS.I/D.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/D.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/D.OR.200(a)(12) 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?	•	

2.1.2 Step 2: Assessment of ISMS implementation is at "Operating" Level (Part-IS compliance)

Reserved for future developments of this policy.

2.1.3 Step 3: Assessment of ISMS implementation is at "Effective" Level

Reserved for future developments of this policy.

2.1.4 Oversight of integrated ISMS and SMS

Reserved for future developments of this policy.

3 Oversight approach by the competent authority

Step 1: Initial ISMS implementation ("Present" and "Suitable")

Organisations should:

- Implement an ISMS at the "Present and Suitable" level by the applicability date of the relevant Part-IS regulation (i.e., 16 October 2025 for organisations covered by Delegated Rule (EU) 2022/1645, and 22 February 2026 for organisations covered by Implementing Regulation (EU) 2023/203, and perform, by that date, a Compliance Monitoring activity to ensure that the organisation meets those requirements.
- Start operating such ISMS immediately after the applicability date.

In order for the competent authority to assess that the organisation has demonstrated that it has implemented an ISMS at "Present and Suitable" level and is ready to operate the ISMS, organisations need to make available sufficiently in advance of the applicability date to their competent authority the following:

1. The first version of their "Information Security Management Manual (ISMM)", which may be integrated with other manuals or expositions already held by the organisation.
2. The procedure described under Part-IS points IS.I/D.OR.255 *"Changes to the information security management system".* This procedure may be part of the ISMM or integrated into an existing change procedure (e.g. according ORO.GEN.130 or similar requirements in other domains).
3. An initial risk assessment identifying:
    a. the organisation's activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains
    b. the equipment, systems, data and information that contribute to the functioning of the elements listed in point (a) above
    c. the interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks
    d. The major risks and related threat scenarios, both internal and at the interfaces with other organisations
4. Evidence that internal compliance monitoring activities have taken place, describing the organisational level of compliance with all the criteria described in the columns "ISMM" and "Audit" of the table in point **"2.2.1 Step 1: Assessment of Basic ISMS implementation ("Present" and "Suitable")"** of this document, identifying any elements where the "Present" and "Suitable" level has not been reached and including a corrective action plan for those elements.

Once such documentation is received, the competent authority should follow a "two-phase approach" in order to assess that the organisation has implemented the ISMS at the level "Present" and "Suitable" and it is ready to operate the ISMS:

- **Phase 1:** Review and approve the ISMM and the procedure described under Part-IS points IS.I/D.OR.255 *"Changes to the information security management system"*, preferably before the applicability date of the rule (see Case 2 and Case 3 below when this is not possible).

  The review of the ISMM should be performed by checking the elements contained in the column "ISMM" of the table in point **"2.2.1 Step 1: Assessment of Basic ISMS implementation ("Present" and "Suitable")"** of this document and may include not only a desktop review of the ISMM, but also discussions and clarifications with the organisation.

  During the review of the change procedure, the competent authority is expected to pay particular attention to the following:

  - The procedure clearly describes the roles and responsibilities of the staff involved in the proposal, analysis, evaluation of impacts, agreement and authorization of the changes.
  - The level of understanding of the organisation of the Part-IS requirements by evaluating the completeness and accuracy of the compliance monitoring activities described in point 4 above and by assessing the relevance of the initial risk assessment provided by the organisation in accordance with point 3 above.

- **Phase 2:** Audit the organisation to assess that they have implemented the ISMS at the level "Present" and "Suitable" and they are ready to operate the ISMS. This audit may be performed after the applicability date of the rule in order for the competent authority to integrate it in any on-going oversight activities of the organisation. This may facilitate the authority to integrate such audit with other audits already planned for other management system requirements (e.g. SMS, NIS Directive, AVSEC Regulation…).

  This review should be performed by checking the elements contained in the column "Audit" of the table in point **"2.2.1 Step 1: Assessment of Basic ISMS implementation ("Present" and "Suitable")"** of this document.

  This audit may combine elements audited onsite and elements audited remotely and may also take the form of assessments and inspections.

Regarding **Phase 1**, and whether it will be possible for the authority to approve such documents before the applicability date, several cases are contemplated considering when the organisation has made available to the competent authority the relevant documentation:

- **Case 1:** The organisation has made available the documentation to their competent authority sufficiently in advance of the applicability date, making possible for the competent authority to approve the ISMM and the procedure described under Part-IS points IS.I/D.OR.255 by the applicability date.
- **Case 2:** The organisation has made available the documentation to their competent authority before the applicability date but has not provided sufficient time to allow the

authority to approve the ISMM and the procedure described under Part-IS points IS.I/D.OR.255 by the applicability date.

In this case, and while the competent authority if still performing the assessment, the organisation may continue operating normally, unless any findings already identified by the authority justify the need for limitations.

- **Case 3:** The organisation has not made available the documentation to their competent authority by the applicability date.

  In this case, the competent authority is expected to raise a Level 2 finding indicating that the organisation has not provided any proof of compliance with ISMS requirements. Depending on the reactivity of the organisation in sending the documents described above, and a preliminary review of the documents (if/when received) the authority may allow the organisation to continue operating normally or may impose limitations, while the Level 2 finding is closed.

Approval of the ISMM:

As required by Part-IS points IS.I/D.OR.250(b) *"Information security management manual (ISMM)"*, the first issue of the ISMM shall be approved by the competent authority.

The administrative method used to grant approval of the ISMM (e.g. official letter, etc) will be decided by each competent authority, possibly following similar procedures already used for the approval of the current manuals and/or expositions held by those organisations.

In those cases where the organisation has integrated the elements of the ISMM in an existing manual/exposition already held by the organisation (e.g. inside the POE for Production Organisations, or inside the MOE for Maintenance Organisations), the approval of the elements related to Part-IS may be granted by approving the revision of the manual/exposition where they have been integrated.

In the case of organisations holding multiple approvals, the elements of the ISMM may be integrated in a single manual/exposition.

Approval of the procedure described under Part-IS points IS.I/D.OR.255 *"Changes to the information security management system"*:

As required by Part-IS points IS.I/D.OR.255(a), this procedure shall be approved by the competent authority.

When approving this procedure, the competent authority is expected to pay particular attention to the following:

- The procedure clearly describes the roles and responsibilities of the staff involved in the proposal, analysis, evaluation of impacts, agreement and authorization of the changes.
- The level of understanding of the organisation of the Part-IS requirements by evaluating the completeness and accuracy of the compliance monitoring activities described in point 4 above and by assessing the relevance of the initial risk assessment provided by the organisation in accordance with point 3 above.

The method used to grant approval of this procedure (e.g. official letter, etc) will be decided by each competent authority.

Steps 2 and 3: ISMS implementation at "Operational" and "Effective" levels

Once the competent authority has assessed that the organisation has reached the "Present and Suitable" levels, the competent authority shall move to plan and perform the assessment of the "Operational" and "Effective" levels of ISMS implementation. This assessment may be integrated in the regular oversight activities.

It is important to note that the organisation will only be deemed to have reached Part-IS compliance once the authority has completed all the phases leading to the authority concluding that organisation has reached the "Present", "Suitable" and "Operating" implementation levels. This assessment process is not expected to be completed until well after the applicability date, since it is necessary for the ISMS to be operating and producing results during a reasonable and sufficient amount of time, the authority needs to perform the appropriate audits, assessments and inspections, and any findings will need to be closed.

4 Proportionality aspects for Part-IS implementation in relation to organisational complexity and safety relevance

As indicated in GM1 IS.I/D.OR.200(d):

“When implementing the processes and procedures, as well as establishing the roles and responsibilities required under point “IS.I/D.OR.200(d)”, the organisation should primarily consider the risks that it may be posing to other organisations, as well as its own risk exposure. Other aspects that may be relevant include the organisation’s needs and objectives, information security requirements, its own processes and the size, complexity and structure of the organisation, all of which may change over time.”

For all organisations, it's critical to strategically manage the effort to match available resources, achieving compliance and ensuring robust protection for those information security risks with potential safety impact. The following guidelines intend to ensure that this is done effectively and proportionately to the complexity of the organisation from an information security perspective.

Since there is no clear distinction between complex and non-complex organisations, when assessing an organisation's complexity in terms of information security, the competent authority should consider each of the following elements separately. Each element, on its own, can influence certain aspects of a proportionate ISMS implementation:

a) **Where the organisation is placed in the functional chain** and the number and safety relevance of the interfacing organisations/stakeholders.
b) The **complexity of the organisational structure and hierarchies** (e.g. number of staff, departments, hierarchical layers, etc)
c) The **complexity of the information and communication technology systems and data** used by the organisation and their connection to external parties.

The above indicators of complexity and their influence on the proportionate implementation of Part-IS are described in the following points.

4.1 Proportionality considerations related to the indicators of complexity and safety relevance

4.1.1 Organisation role in the functional chain and number and criticality of interfacing organisations/stakeholders

The organisation's position in the functional chain and its overall contribution to the safety of related functional processes are key indicators of complexity. This has a direct influence on the depth of risk assessment required and the level of assurance needed to ensure the effectiveness of measures implemented to mitigate unacceptable risks.

When assessing organisations whose **position in the functional chain and its interfaces does not pose a risk of unsafe conditions**, the following approaches should be considered acceptable:

a) Risk Assessment and Treatment

- **Simplified Risk Assessment**: A streamlined risk assessment process that prioritises risks based on their potential impact on safety is used. The assessment focuses on high-impact areas and applies more detailed assessments only where and if necessary.
- **Risk Treatment Prioritisation**: A risk treatment plan that prioritises addressing high-impact risks with cost-effective measures is 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.

In turn, when assessing organisations whose **position in the functional chain and its interfaces may create a risk of unsafe conditions**, the following approaches should be expected:

a) Risk Assessment and Treatment

- **Detailed Risk Assessments:** Detailed and often more frequent risk assessments are carried out.

4.1.2 Complexity of the organisational structure, hierarchies and processes

The complexity of an organisation's structure—typically determined by the number of staff, hierarchical layers, number of processes and their interdependences—directly influences the level of internal coordination required and the extent to which information exchange needs to be formalised and proceduralised.

When assessing organisations characterised by a **combination of limited number of staff members, few hierarchical layers and straight forward processes**, the following approaches should be accepted:

a) Policy and Procedure Simplification:

- **Streamlined documentation:** Policies and procedures are concise, clear and easy to understand. Overly complex documents are avoided to ensure the usability by a small team. Templates and frameworks may have been used in order to speed up the creation of necessary documentation.
- **Focus on key policies:** The development has been prioritised on the key policies in order to address the most critical aspects of information security, such as management commitment, access control and incident response.

b) Employee Training and Awareness:

- **Targeted Training Programs**: Focused training programs that target the specific roles and responsibilities of employees has been provided. The training should be relevant to the organisation's specific risks and operational context.
- **Security Culture:** A culture of security awareness is encouraged throughout the organisation. Regular, short training sessions and awareness campaigns are conducted.

c) Outsourcing and Partnerships:

- **Outsourcing**: For areas where the organisation lacks expertise, outsourcing to managed security service providers is adopted.
- **Collaboration with Peers:** Information-sharing with similar organisations (e.g. through ECCSA, the European Centre for Cybersecurity in Aviation) or industry groups is carried out. Collaboration provides insights to evaluate the evolution of the security environment with limited effort.

d) Engagement with Management:

- **Simplified Management Reporting:** Reports to management are concise, and focused on key metrics that demonstrate the effectiveness of the ISMS. Continued support and resource allocation from top management is ensured.

e) 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 should be on the most critical areas and the audit results should be provided to the Accountable Manager and utilised to guide continuous improvement.

- **Agile Review Process**: The ISMS should be regularly reviewed and, if necessary, adapted to ensure that it remains aligned with the organisation's evolving needs and threats.

In turn, when assessing organisations characterised by a **combination of large number of staff members, hierarchical layers and a high number of interconnected processes and interfaces** the following approaches should be expected:

a) Robust Governance Structure:

- **Information Security Governance Committees**: Governance committees to oversee the ISMS should be present, to ensure alignment with the organisation's safety and security objectives. These committees should include representation from senior management, IT, legal, and key business units.
- **Metrics and Reporting**: Comprehensive metrics and reporting structures to track the effectiveness of the ISMS should be implemented. Report on key performance indicators

(KPIs) to senior management and the board should be provided to ensure ongoing support and resource allocation.

b) Extensive Policy and Procedure Framework:

- **Detailed Policies and Procedures**: More complex organisations need a more extensive set of policies and procedures to cover various business units, compliance requirements, and operational processes. This includes specialized policies for areas like cloud security, third-party management, and mobile device management.
- **Policy Harmonization**: Ensure that policies are harmonized across the organisation to avoid conflicting practices between different departments or regions. This requires a centralized governance model to oversee policy development and enforcement.

c) Risk Assessment and Treatment:

- **Cross Risk Assessments:** Risk assessments includes assessing risks across various departments, geographic locations, and technological platforms.
- **Risk Aggregation and Correlation**: With a larger volume of information, risks assessments should be aggregated and correlated to identify systemic issues and ensure that risks are managed and escalated at an organisational level, not just within individual silos.

d) Comprehensive Training and Awareness Programs:

- **Role-Based Training**: Extensive role-based training programs tailored to different functions within the organisation is implemented. For example, IT staff, executives, and end-users all have different levels of training specific to their roles.
- **Continuous Security Awareness Campaigns**: Security awareness campaigns using various methods (e.g., phishing simulations, workshops, e-learning modules) are continuously deployed to keep security top-of-mind for all employees across the organisation.

e) Enhanced Contracted Activities Management:

- **Supply Chain Risk Management**: Thorough security assessments of contracted organisations and ongoing monitoring of third-party risks should be carried out. Security requirements should be integrated into contracts.
- **Third-Party Audits**: Regular audit of contracted organisations should be done in order to ensure they comply with the organisation's security objectives.

f) Comprehensive Incident Management

- **Dedicated Security Operations Centre (SOC)**: A dedicated SOC should be established in order to monitor security events 24/7, manage incidents, and coordinate response efforts across the enterprise.

- **Complex Incident Response Plans**: A detailed incident response plans that cover a variety of scenarios, including cross-departmental coordination, communication strategies, and operational continuity planning should be developed and maintained.

- **Crisis Simulation Exercises**: Crisis simulation exercises that involve key stakeholders across the organisation are regularly conducted to test the effectiveness of incident response and operational continuity plans.

g) Continuous Improvement and Compliance Monitoring Programs

- **Internal and External Audits**: Comprehensive internal audits are regularly conducted to assess compliance with the ISMS and identify areas for improvement.
- **Continuous Improvement Programs**: A continuous improvement process to update and refine the ISMS based on audit findings, incident post-mortems, and changes in the threat landscape is implemented.

4.1.3 Complexity of the 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.

When assessing organisations characterised by a **combination of usage of few ICT tools and utilisation of standard ICT products in a basic, commercial of-the-shelf, ICT-architecture**, the following approaches should be accepted:

a) Use of Standards and Tools

- **Leverage ISO/IEC 27001 Controls**: Usage of the ISO/IEC 27001 Annex A controls as a checklist to ensure all critical areas are covered while reducing the effort of designing controls from scratch. In such cases the Part-IS vs. ISO/IEC 27001 comparison guide shall be referenced to ensure that Part-IS specifics have been correctly addressed.
- **Simplified Incident Management: A** basic incident management process that allows for quick identification, reporting, and response to security incidents is adopted. Lessons learned from incidents should be anyhow integrated into the ISMS for continuous improvement.
- **Automated Tools**: Automated tools for monitoring, logging, and managing security incidents are used in order to reduce manual effort while maintaining continuous compliance.

b) Documentation and Record Keeping

- **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, version control, and ensure the security of records.

In turn, when assessing organisations characterised by a **combination of usage of several and diverse ICT tools, amongst which bespoke ICT solutions and architectures**, the following approaches should be expected:

a) Advanced Security Technologies

- **Integration of Advanced Security Tools**: Security technologies like Security Information and Event Management (SIEM), Data Loss Prevention (DLP), and Endpoint Detection and Response (EDR) systems should be utilised to help manage the scale and complexity of monitoring, detecting, and responding to security incidents across the organisation.
- **Automated Threat Intelligence**: Automated threat intelligence platforms should be implemented to enable real-time threat detection and response across the broad threat surface.

b) Extensive Record Keeping and Documentation

- **Detailed Documentation**: An extensive documentation of all ISMS processes, risk assessments, incident reports, and compliance activities is carried out.
- **Record Retention**: Record and data are widely collected, retained and securely stored and accessible over extended periods.