Assessment of ISMS implementation at "Present" and "Suitable" levels

Relevance of different requirements with respect to the foundation of ISMS

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

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

PROCEDURES IMPLEMENTATION VERFICATION

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).
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

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

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	a) Has the structure been updated to reflect the ISMS (e.g. appointment of an information security manager, reporting structure)?	•	
	o 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?	•	•
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			

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	a) Has the organisation developed a clearly defined information security policy?	•	
	o Is the purpose of the policy clearly stated?	•	
	o Are the information security objectives defined?	•	
	o Is the concept of aviation safety an integral part of the policy?	•	
	o Is the content of the policy appropriate to the complexity of the organisation?	•	•
	o 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?	•	•
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
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)? •	•	
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
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?	•	
	c) Has the organisation ensured appropriate access of the Competent Authority to the contracted parties and included this in the corresponding contracts?	•	•
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			
IS.I.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?	•	•
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I.OR.205 and 210 Risk management	a) Has a formal process for information security risk management been established?	•	
	o Are there the three main processes or procedures (i.e. Risk identification, Risk assessment and Risk treatment) defined within the risk management context?	•	
	o 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) ?	•	
	e) Has the organisation already included the applicable assets in the inventory?		•
	f) Has a formal process for information security risk management been established?		•
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I.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?		•
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I.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?	•	
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			

Regulatory requirements	Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS)	ISMM review	Audit
IS.I.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.)	•	•
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			
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?	•	
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			

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)(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? •	•	
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			
IS.I.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?	•	
Reviewed Items/Comments/Findings			
Assessment Classification **PRESENT** ☐ **SUITABLE** ☐			

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.