Minimum Essential Requirements for the Oversight & Management of Internal ISMS Responsible Person and External IT Subject Matter Expert.

Sofema Online (SOL) considers the functional process to manage Information Security & Cyber within a typical small EASA Part 145 Organisation

Introduction The appointed ISM person should be an internal member of the management structure and have the authority to ensure compliance, specifically:

- **Authority & Reporting:** They must be appointed by the Accountable Manager and report to them (or a delegated person), ensuring they have the necessary corporate authority to establish and maintain the ISMS, allocate resources, and support the objectives described in Information Security (Regulations (EU) 2023/203.
- **Competence:** They must possess the appropriate knowledge, background, and experience to fully understand the requirements of this Regulation and oversee the ISMS. This includes understanding the risks inherent in the contracted activities.
- **Oversight of Outsourced Activities (IS.I.OR.235):** This is a critical function. They must ensure that the contracted activities comply with the Regulation and that the service provider works under the organisation's oversight. They are also responsible for ensuring the competent authority can have access to the contracted organisation upon request.
- **Compliance Monitoring:** They must manage the compliance monitoring function for the ISMS, providing feedback to the accountable manager for implementing corrective actions. Crucially, they must ensure the independence of this monitoring function, even if they hold multiple roles in the organisation.

Task List: Focus on Management, Oversight, and Compliance

This task list focuses on the core duties your internal IS Responsible Person must perform, keeping in mind the external nature of your operational IT support.

1. Governance and Documentation Management

Task Area	**Key Activities for Internal IS Responsible Person**	Part-IS Reference
ISMS Foundation	Define and document the scope of the ISMS (all systems/data impacting aviation safety).	IS.I.OR.205(a)
Policy & Manual	Establish and promote the Information Security Policy (approved by the Accountable Manager).	IS.I.OR.200(a)(1)
	Create and maintain the ISMM (Information Security Management Manual) and procedures, integrating with other manuals (e.g., MOE, CAME) where applicable.	IS.I.OR.250
Staffing & Competence	Maintain a process for managing personnel competence, addressing identified knowledge gaps, and ensuring relevant training.	IS.I.OR.240(g)
	Ensure all personnel acknowledge their assigned IS responsibilities.	IS.I.OR.240(h)

2. Risk Management and IS Activities Oversight

Task Area	Key Activities for Internal IS Responsible Person	Part-IS Reference
Risk Assessment	**Identify all internal IS risks** and risks from **external interfaces** (including the external IT provider) that could impact aviation safety.	IS.I.OR.205(a), (b)

Task Area	Key Activities for Internal IS Responsible Person	Part-IS Reference
	Coordinate with the external IT provider to acquire necessary risk information for an accurate assessment of **shared risks**.	IS.I.OR.205(c)
Risk Treatment	Define **risk treatment measures** for unacceptable risks and ensure the **external IT provider implements their assigned controls** in a timely manner.	IS.I.OR.210(a)
Risk Review	**Review and update the risk assessment** based on defined intervals, changes in operations, and feedback from the IT provider (e.g., changes in the services or risks they communicate).	IS.I.OR.205(d)

3. Management of External IT Services (Contracted Activities)

Task Area	Key Activities for Internal IS Responsible Person	Part-IS Reference
Supplier Vetting	Conduct a **prior assessment of the external IT provider's** competence, suitability, and qualifications related to the IS activities being contracted.	AMC1 IS.I.OR.235(a)(b)
Contractual Oversight	Maintain a **structured process to oversee the contract**, including defining the scope, roles/responsibilities, and **reviewing performance metrics (KPIs)**.	AMC1 IS.I.OR.235(a)
Incident Reporting	Ensure the **contract requires the external IT provider to report all IS events/incidents** to the organisation, especially those which may lead to an unsafe condition.	IS.I.OR.215(c)

Task Area	Key Activities for Internal IS Responsible Person	Part-IS Reference
Audit Rights	Ensure the contract includes a clause granting the **competent authority access** to the external IT provider for compliance checks.	IS.I.OR.235(b)
Compliance Audits	Plan and conduct **compliance audits** of the external IT provider (limited to the contracted IS activities) and follow up on any findings.	AMC1 IS.I.OR.235(a)

4. Incident and Continuous Improvement Cycle

Task Area	Key Activities for Internal IS Responsible Person	Part-IS Reference
Internal Reporting	Manage the internal reporting scheme to identify, correlate, and evaluate all IS events/vulnerabilities received from internal staff *and* the external IT provider.	IS.I.OR.215(a), (b)
Response & Recovery	**Define the organisation's response and recovery procedures** (working closely with the external IT provider on execution where needed) to ensure a safe state is reached within a defined **recovery time**.	IS.I.OR.220(b), (c)
External Reporting	**Report significant risks/incidents** (those posing a **significant risk to aviation safety**) to the competent authority as soon as the condition is known, and submit the full report within **72 hours**.	IS.I.OR.230(b), (c)

Task Area	Key Activities for Internal IS Responsible Person	Part-IS Reference
Compliance Monitoring	Manage the function that **monitors overall compliance** with the Regulation and related procedures (internal audit/assessment).	IS.I.OR.200(a)(12)
Continuous Improvement	Assess the **effectiveness and maturity** of the ISMS and drive necessary improvements (corrections and corrective actions) based on audit results, incident analyses, and risk review.	IS.I.OR.260(a), (b)

Duties for the External IT Subject Matter Expert

1. Technical Risk & Control Implementation

- **Effectiveness Verification:** Conduct activities like penetration testing, vulnerability scanning, and red-team/blue-team exercises to verify the initial and continued effectiveness of implemented security controls.
- **Secure Infrastructure Provision:** Provide and maintain a secure data centre (as a service) or other technical hosting solutions, ensuring records and systems are protected against damage, alteration, and theft.
- **Configuration Management:** Implement and manage security configurations for all systems and equipment within the ISMS scope (e.g., servers, network devices, and End-User devices).

2. Monitoring, Detection, and Response Execution

- **Detection Measures:** Define, develop, and implement the technical measures required to detect information security events that could impact aviation safety. This involves continuous technical monitoring.
- **Vulnerability Discovery & Management:** Actively engage in vulnerability discovery (scanning, patching, testing) and provide an up-to-date list of vulnerabilities affecting contracted systems and services for the internal team to monitor.

- **Incident Response Execution:** Execute the predefined measures and courses of action to respond to detected events and incidents, including controlling the failure mode and containing the spread of any attack.
- **Recovery Actions:** Implement measures aimed at recovering from information security incidents, including necessary emergency measures, to restore systems to a safe and secure state within the defined recovery time.

3. Reporting and Documentation Support

- **Event Reporting (Contractual Obligation):** Report all information security events, incidents, and vulnerabilities to the internal IS Responsible Person in a timely manner (as defined in the contract), especially those which could lead to unsafe conditions.
- **Records Provision:** Provide data, logs, and evidence of IS management activities, including security data files for monitoring and records updates, to the internal IS Responsible Person for archiving and traceability.
- **Documentation Support:** Produce technical procedures that detail the configuration and operation of the security controls and processes implemented under their service contract.

4. Personnel and Compliance Support

- **Personnel Checks:** Perform pre-employment checks (if contracted to do so) to support the organisation's process for establishing the identity and trustworthiness of personnel who have access to information systems and data.
- **Training Delivery:** Define, develop, and deliver adequate training to ensure their own staff performing contracted duties achieve the necessary competence.
- **Compliance Audit Cooperation:** Cooperate fully with the internal IS Responsible Person during compliance audits, providing access to relevant processes, resources, and data, as stipulated in the contract.
- **Immediate Measures:** Implement the immediate reaction measures communicated by the organisation after notification from the competent authority regarding a security incident or vulnerability.

Competence Required for the External IT Subject Matter Expert

The external IT SME needs a mix of deep technical skills to execute the contracted IT security tasks and a foundational understanding of the regulatory context to support the internal IS Responsible Person effectively.

1. Information Security Technical Expertise

- **Vulnerability Management:** Deep technical skill in performing security testing, such as penetration testing, vulnerability scanning, and red/blue team exercises. This includes the ability to accurately identify, analyze, and report vulnerabilities and security control effectiveness.
- **Security Architecture & Implementation:** Expertise in defining, developing, and implementing complex technical security measures and controls (e.g., access controls, encryption, intrusion detection systems) to treat identified risks.
- **Security Monitoring & Detection:** Competence in designing, deploying, and operating technical monitoring systems (like SIEM or logging solutions) to continuously detect deviations and information security events that could impact aviation safety.
- **Incident Response & Forensics:** Technical skills in executing predefined incident response and containment strategies, including identifying the spread of an attack, and performing actions to control system failure modes.

2. IT Operations and Infrastructure Management

- **Infrastructure Provisioning & Hardening:** Proficiency in providing and maintaining secure infrastructure (e.g., cloud services, data centers) and implementing security configurations for various assets like servers, network devices, and end-user devices.
- **Business Continuity/Disaster Recovery (BC/DR):** Expertise in implementing and testing recovery actions and emergency measures to ensure systems can be restored to a safe and secure state within a defined recovery time.
- **Data Integrity & Archiving:** Knowledge of data management practices to ensure that security records, logs, and evidence provided to the organisation for archiving meet requirements for integrity, authenticity, and protection against damage or theft.

- **Configuration Management:** Technical ability to reliably implement and manage security configurations across all contracted IT systems and equipment within the ISMS scope.

3. Aviation/Regulatory Support Competence

- **Aviation Context Awareness:** Foundational knowledge of the high-level aviation safety context, particularly relating to how IT events (incidents/vulnerabilities) can quickly evolve into conditions that pose a significant risk to aviation safety. This awareness ensures proper prioritization and reporting.
- **Contractual/Audit Compliance:** Understanding of contractual obligations and the need for transparency, including cooperating fully with compliance audits and ensuring the competent authority is granted necessary access as required by the Part-145 organisation.
- **Reporting Discipline:** Strict adherence to timely reporting procedures for all IS events, vulnerabilities, and incidents to the internal IS Responsible Person, using the contractually defined means.