Implementing Part IS within your EASA Part 145 Organisation

Implementation Timeline Guide Provided by Sofema Aviation Services (SAS)
www.sassofia.com

Introduction

Only 14 months remain until the cut of date of February 22, 2026 by which time all applicable organisations shall be able to demonstrate compliance with **EASA Regulation (EU) 2023/203**

Within this Document - we provide a timeline guide which will take a minimum of 11 Months to address all areas and issues.

Implementing the **information security requirements** within an EASA Part 145 organization's Safety Management System (SMS) requires integrating **Part IS (Information Security)** standards into the existing framework. Below is a structured plan and timeline to achieve compliance.

Timeline for Integration

Immediate Actions (0–3 Months)

Initial Preparation - Regulatory Understanding:

- Review **EASA Regulation (EU) 2023/203** and **Part-IS requirements**, focusing on:
  - **ISMS (Information Security Management System)**.
  - **Integration into existing SMS**.
- Assess overlaps with ISO 27001 or equivalent standards if already implemented.

Notes - Key components of ISMS under EASA include:

- **Risk assessment processes** (aligned with Part IS.I.OR.205).
- **Incident reporting schemes** (internal and external as per Part IS.I.OR.215 and IS.I.OR.230).
- **Record-keeping** for information security incidents and risk management activities.

Integration into Existing SMS

- Integration ensures a seamless approach to managing both safety and information security risks.
- Align ISMS with the SMS framework by embedding:
    - **Risk management practices** to cover both operational and information security risks.
    - A unified **incident response mechanism** that addresses information security breaches within the context of overall organizational safety.
    - **Training and communication protocols** to bridge knowledge gaps and foster a culture of security awareness.
- Synchronize documentation, such as updating the **Maintenance Organization Exposition (MOE)** to include ISMS policies and processes.

Gap Analysis - Compare current SMS practices against the information security requirements.

- Identify vulnerabilities in current processes, particularly in IT systems, data handling, and reporting.

Notes - **Assess Existing SMS Practices**

- Review the **current state** of your SMS, including:
    - **Policies and Procedures**: How are safety risks currently managed? Are there provisions for managing information security risks?
    - **Risk Management Framework**: What is the process for identifying, assessing, and mitigating risks?
    - **Incident Reporting**: How are incidents reported, tracked, and resolved? Is there an existing system for handling security breaches?

Map Part-IS Requirements

- Examine the specific requirements of **EASA Regulation (EU) 2023/203** and Part-IS, including:
    - **Risk Management** (Part IS.I.OR.205).
    - **Incident Detection, Response, and Recovery** (Part IS.I.OR.215).

  - **Reporting Mechanisms** (Part IS.I.OR.230).
  - **Continuous Improvement** (Part IS.AR.235).

Compare Current Practices

- Identify areas where your existing SMS addresses information security requirements.
- Highlight gaps where additional controls or processes are required

Team Formation:

  - Establish an **Information Security Taskforce**, involving SMS managers, IT security specialists, and compliance officers.

Short-Term Actions (4–6 Months)

Planning - Define Objectives - Set clear goals for integrating information security into the SMS, including risk management and incident response.

Key Goals:

- **Align Information Security with SMS Priorities:**
  - Ensure that information security is treated as a core component of overall safety management.
  - Develop objectives that prioritize aviation-specific threats, such as:
    - Cyberattacks targeting operational IT systems.
    - Unauthorized access to safety-critical data.
    - Compromise of communication systems.
- **Establish a Culture of Security Awareness:**
  - Build organizational awareness of information security risks through training and communication.
  - Promote a shared responsibility for information security across all departments and personnel.
- **Meet Regulatory and Industry Standards:**

  - Ensure compliance with EASA Regulation (EU) 2023/203 and Part-IS requirements.
  - Integrate best practices from ISO 27001 and other relevant information security frameworks.

SMART Objectives:

When defining goals, use the **SMART** criteria:

- **Specific**: Clearly define what the organization aims to achieve (e.g., "Develop an ISMS framework integrated into SMS by Month 6").
- **Measurable**: Set quantifiable targets (e.g., "Train 100% of staff on incident response procedures").
- **Achievable**: Ensure goals are realistic given the organization's resources and timeline.
- **Relevant**: Align objectives with regulatory requirements and operational needs.
- **Time-bound**: Assign deadlines to each objective (e.g., "Complete risk assessment by the end of Month 5").

Information Security Risk Assessment:

  - Conduct a comprehensive **Information Security Risk Assessment** in line with Part IS.I.OR.205.
  - Prioritize risks with potential safety impacts.

1. **Select a Methodology**:
    - Use a recognized risk assessment methodology, such as:
        - **ISO 27005** for information security risk management.
        - **NIST Risk Management Framework (RMF)**.
    - Tailor the methodology to address aviation-specific risks and Part-IS requirements.

Gather Relevant Data:

  - Collect documentation on existing systems, procedures, and previous security incidents.

    - Review regulatory requirements and guidance material (e.g., EASA AMC and GM to Part IS.I.OR.205).

Risk Identification

Objectives:

- Identify potential threats and vulnerabilities in systems, processes, and assets.

Key Activities:

- **Asset Inventory**:
    - List critical assets that require protection, such as:
        - Maintenance records and operational data.
        - IT systems (e.g., maintenance planning software, ERP systems).
        - Physical infrastructure (e.g., server rooms, network equipment).
- **Threat Identification**:
    - Identify potential threats, including:
        - **Cyber Threats**: Malware, ransomware, or phishing attacks.
        - **Insider Threats**: Unauthorized access or accidental data breaches.
        - **Environmental Threats**: Power outages, natural disasters, or hardware failures.
- **Vulnerability Assessment**:
    - Examine weaknesses in current controls or processes, such as:
        - Lack of multi-factor authentication.
        - Outdated software with known vulnerabilities.
        - Inadequate staff training on cybersecurity best practices.
- **Mapping Threats to Assets**:
    - Link identified threats to specific assets and systems to understand their potential impact.

Risk Evaluation - Objectives:

- Assess the likelihood and impact of identified risks to prioritize mitigation efforts.
- **Assess Likelihood**:
    - Evaluate the probability of a threat exploiting a vulnerability.
    - Use historical data, expert opinions, or industry trends to estimate likelihood.
- **Assess Impact**:
    - Determine the potential consequences of a security incident, including:
        - **Operational Impact**: Downtime or loss of critical systems.
        - **Safety Impact**: Threats to aviation safety or passenger security.
        - **Financial Impact**: Costs associated with data breaches or regulatory penalties.
- **Develop a Risk Matrix**:
    - Combine likelihood and impact scores to categorize risks as:
        - Low: Acceptable with minimal controls.
        - Medium: Requires mitigation to reduce risk.
        - High: Critical and needs immediate attention.
- **Documentation**:
    - Update the Maintenance Organization Exposition (MOE) to include information security management processes.
    - Develop an **Information Security Management Manual (ISMM)**.

Training

- Design training programs to educate all staff on:
    - Information security basics.
    - Identifying and reporting security events.
    - New reporting and incident management procedures.

Notes - Regulatory Basis for Training

EASA’s Part-IS requirements emphasize that personnel involved in safety-critical tasks must be adequately trained to identify and manage information security risks. This includes understanding the organization’s Information Security Management System (ISMS) and contributing to the detection, reporting, and mitigation of information security incidents.

Relevant Part-IS Sections:

- IS.I.OR.225 - Personnel Requirements: Organizations must ensure that all personnel have the necessary competence to perform their duties in compliance with information security requirements.
- IS.I.OR.215 - Incident Reporting: Staff must be trained to recognize and report security incidents that could impact safety.

Training Program Design - Key Training Objectives

- Foster a basic understanding of information security principles.
- Equip staff to identify potential information security events and understand their significance to aviation safety.
- Ensure all employees know how to report incidents internally and externally.
- Provide specific training tailored to the roles and responsibilities of individual staff members.

Training Topics

- Information Security Basics - To create a foundational understanding of information security concepts and their importance in aviation.
- What is Information Security?
    - Key principles: confidentiality, integrity, and availability of data.
    - Relevance to aviation safety and compliance.
- Types of Threats:
    - Cyber threats (e.g., phishing, ransomware, data breaches).
    - Insider threats (accidental or intentional data compromise).
    - Physical threats (loss of devices, unauthorized access to IT systems).

- Role of Employees in Information Security:
  - Basic responsibilities for protecting sensitive data.
  - Overview of the ISMS and its relevance to daily tasks.

Delivery Format - Classroom or virtual sessions for all staff.

- Simplified materials for non-technical roles to ensure accessibility.

Identifying and Reporting Security Events To empower employees to act as the first line of defense in identifying and responding to potential information security risks.

- Recognizing Security Events:
  - Unusual system activity (e.g., unexpected logins, slow performance).
  - Signs of phishing (e.g., suspicious emails or links).
  - Physical breaches (e.g., unauthorized personnel accessing secure areas).
- Understanding Event Impacts:
  - How security events can escalate to incidents affecting aviation safety.
  - Examples of past events and their outcomes (case studies).
- Reporting Protocols:
  - Internal processes: who to notify, how, and when.
  - Using reporting tools or forms provided by the organization.

Delivery Format - Role-specific workshops (e.g., IT staff, maintenance personnel, and administrative staff). Hands-on activities, such as identifying phishing attempts in simulated scenarios.

New Reporting and Incident Management Procedures - Purpose: To ensure compliance with Part IS.I.OR.215 and Part IS.I.OR.230, organizations must train staff on internal and external reporting mechanisms.

- Internal Reporting:
  - Chain of command for escalating information security concerns.
  - Using internal reporting systems (e.g., ticketing tools, dedicated hotlines).
  - Required documentation (e.g., incident logs, immediate actions taken).

- External Reporting:
    - Regulatory requirements for notifying EASA or other competent authorities.
    - Understanding the criteria for reportable incidents.
    - Timelines and procedures for external reporting.
- Incident Management:
    - Overview of the organization's incident response plan.
    - Staff roles during incidents (e.g., containment, mitigation, communication).
    - Post-incident reviews and lessons learned.

Delivery Format - Interactive modules for all staff with organization-specific examples - Targeted training for incident response teams or those responsible for regulatory reporting.

Role-Specific Training

In addition to general training, specific groups within the organization require tailored instruction based on their roles and responsibilities:

Role	Training Focus
Senior Management	Strategic understanding of Part-IS requirements and their impact on business continuity and compliance.
IT and Cybersecurity	Advanced technical training on identifying, managing, and mitigating cybersecurity risks.
Maintenance Staff	Practical training on identifying physical threats to IT systems or data during maintenance operations.
Administrative Staff	Focused on handling sensitive data securely and recognizing suspicious activities in daily operations.
Incident Response Team	Comprehensive instruction on containment, root cause analysis, and recovery protocols during incidents.

Delivery Methods - To ensure accessibility and effectiveness, training should leverage a combination of delivery methods:

- Classroom Sessions: In-person or virtual sessions for foundational topics.
- E-Learning Modules: Self-paced courses for general and role-specific training.
- Workshops and Drills: Hands-on exercises, such as simulated phishing attacks or mock incident response scenarios.
- On-the-Job Training: Practical guidance during regular operations for context-specific learning.

Frequency of Training - To maintain compliance and adapt to evolving threats:

- Conduct initial training for all staff upon implementing the ISMS.
- Schedule refresher training annually or after significant updates to the ISMS or regulatory requirements.
- Provide ad hoc training following specific incidents or changes in the threat landscape.

Evaluation and Continuous Improvement - Regular evaluation ensures the training program remains effective:

- Knowledge Assessments: Test staff understanding through quizzes or practical demonstrations.
- Feedback Mechanisms: Gather participant feedback to refine training materials.
- Performance Monitoring: Use metrics such as incident reporting rates or audit findings to gauge training success.

Implementation Phase (7–12 Months) - Operational Integration

Implement ISMS:

- Establish processes for continuous **monitoring, detection, and response** to information security incidents.
- Introduce secure access controls and monitoring for sensitive systems.

Notes - The **Implementation Phase** focuses on embedding the **Information Security Management System (ISMS)** into the organization’s operational framework. This involves creating robust processes and controls to monitor, detect, and respond to security incidents while securing access to critical systems. The goal is to align with EASA Regulation (EU) 2023/203 and ensure operational resilience.

Establish Processes for Continuous Monitoring, Detection, and Response

Continuous Monitoring

Continuous monitoring is essential for identifying vulnerabilities, detecting threats, and maintaining the integrity of sensitive systems.

Key Activities:

Deploy Monitoring Tools:

- Implement **Security Information and Event Management (SIEM)** systems to aggregate and analyze security event data in real time.
- Use **Network Monitoring Systems (NMS)** to detect unusual traffic patterns or unauthorized access attempts.
- Apply **Endpoint Detection and Response (EDR)** tools to monitor devices connected to the network.
- **Define Monitoring Parameters:**
    - Identify critical systems and data that require constant oversight.
    - Establish baseline activity levels to detect anomalies.
- **Automate Alerts:**
    - Configure automated alerts for events like:
        - Unusual login patterns (e.g., multiple failed attempts).
        - Access outside working hours or from unrecognized locations.
        - Unauthorized changes to critical system configurations.
- **Conduct Regular Reviews:**
    - Analyze monitoring data for patterns indicative of emerging threats.
    - Schedule periodic audits to validate the effectiveness of monitoring tools.

Incident Detection - Proactive detection ensures swift identification of information security events that could escalate into incidents.

Key Activities:

- **Develop Detection Protocols:**
    - Define criteria for classifying events as potential security incidents.
- **Simulate Threat Scenarios:**
    - Conduct mock attack scenarios, such as simulated phishing campaigns or penetration tests, to test the organization's detection capabilities.
- **Empower Employees -** Train staff to recognize suspicious activity, such as:
        - Unexpected emails with attachments or links.
        - Unusual system behavior during routine tasks.
        - Alerts from antivirus or other security tools.

Incident Response - A clear and efficient response mechanism minimizes the impact of security incidents.

Key Activities:

- **Develop an Incident Response Plan (IRP):**
    - Define roles and responsibilities for all team members involved in responding to incidents.
    - Include detailed steps for containment, investigation, mitigation, and recovery.
- **Establish a Communication Protocol:**
    - Set up an internal reporting mechanism (e.g., hotline or incident reporting software).
    - Define external reporting requirements, ensuring compliance with **Part IS.I.OR.215 and IS.I.OR.230** for notifying competent authorities.
- **Test the Response Plan:**
    - Conduct regular drills to validate the IRP’s effectiveness.

  - Include scenarios that reflect real-world threats, such as ransomware attacks or data breaches.

- **Post-Incident Reviews:**
  - After resolving an incident, conduct a **root cause analysis** to identify gaps in controls.
  - Update the ISMS based on lessons learned to prevent recurrence.

Introduce Secure Access Controls and Monitoring for Sensitive Systems

Access Controls - Effective access controls restrict unauthorized users from accessing sensitive systems or data, a critical requirement under Part-IS.

- **Implement Role-Based Access Control (RBAC):**
  - Grant system access based on the principle of **least privilege**.
  - Define roles clearly and limit access to only those resources necessary for a user’s duties.
- **Enable Multi-Factor Authentication (MFA):**
  - Require users to verify their identity through multiple factors (e.g., password and mobile OTP).
  - Use MFA for all sensitive systems, including maintenance management software and operational databases.
- **Monitor Privileged Accounts:**
  - Track activities of users with elevated privileges (e.g., administrators) to ensure compliance.
  - Use tools to log and audit their actions.
- **Enforce Password Policies:**
  - Require complex passwords with regular updates.
  - Use password managers to reduce the risk of weak or reused credentials.

System Monitoring

Monitoring critical systems ensures real-time visibility and control over potential vulnerabilities.

Key Activities:

- **Track System Activity:**
  - Use logging tools to record user activity across systems.
  - Retain logs for sufficient periods to support forensic investigations.
- **Conduct Vulnerability Scans:**
  - Regularly scan systems for known vulnerabilities using automated tools.
  - Prioritize and address vulnerabilities based on their severity and impact.
- **Segment Networks:**
  - Divide networks into segments to limit the spread of potential threats.
  - Apply stricter controls to segments housing sensitive systems.
- **Secure Physical Access:**
  - Restrict access to server rooms and network equipment.
  - Use badge systems, biometric access, or video surveillance for sensitive areas.

Documentation and Reporting

Comprehensive documentation ensures transparency and facilitates regulatory compliance:

- **ISMS Manual Updates:**
  - Document processes for monitoring, detection, and response.
  - Include access control policies and monitoring procedures.
- **Incident Logs:**
  - Maintain detailed logs of all security events and incidents.
  - Ensure logs are available for audits and regulatory review.
- **Reporting Templates:**

  - Standardize templates for reporting incidents to EASA and other authorities.

Expected Outcomes

By the end of the implementation phase, your organization will:

1. Have established **proactive monitoring and detection mechanisms** for information security threats.
2. Implement **secure access controls** to protect sensitive systems and data.
3. Possess a **tested and validated incident response plan**.
4. Ensure compliance with **EASA Regulation (EU) 2023/203** and the integration of Part-IS requirements into operational processes.

- Create an **internal and external reporting scheme** in compliance with Part IS.I.OR.215 and IS.I.OR.230.

Testing and Validation

- Perform **mock exercises** to test the new information security elements, such as:
  - Incident detection and response protocols.
  - Communication during a breach.
- Validate that procedures align with safety objectives and SMS goals.

Continuous Improvement (12+ Months and Beyond) - Full Operationalization

- **Audit and Review**:
  - Conduct internal audits to ensure all processes comply with Part IS.
  - Engage with the competent authority for feedback and adjustments.
- **Data Analytics**:
  - Use data from monitoring and incident logs to refine risk treatment strategies.

Recertification and Updates

- Prepare for regular oversight and updates as required by **Part IS.AR.235 Continuous Improvement**.

- Stay updated on future amendments to EASA regulations or cybersecurity standards.

Overall Timeline Summary

Milestone	**Timeline**	**Key Activities**
Initial Preparation	0–3 months	Gap analysis, team formation, regulatory review
Planning	4–6 months	Define objectives, risk assessment, documentation
Implementation	7–12 months	ISMS deployment, incident reporting, training
Continuous Improvement	12+ months	Audits, refinement, recertification

With the February 22, 2026, compliance deadline fast approaching, implementing EASA Regulation (EU) 2023/203 requirements within your EASA Part 145 organization demands immediate and sustained action. By adhering to the structured timeline outlined in this guide, organizations can ensure a systematic integration of Part IS standards into their SMS, enhancing information security resilience and regulatory alignment.

Starting now, with a focus on preparation, planning, implementation, and continuous improvement, your organization can achieve compliance within the necessary timeframe, positioning itself not only to meet regulatory obligations but also to strengthen overall operational safety and security. Sofema Aviation Services (SAS) is here to support your journey to compliance, ensuring a seamless transition to meet these critical requirements.

Next Steps

Please email Team@sassofia.com to discuss how we can support your Part IS Integration