EASA Part 145 Cyber Security Implementation Frequently Asked Questions

1. What is Regulation (EU) 2023/203, and how does it impact EASA Part 145 organizations?

- Regulation (EU) 2023/203 mandates that EASA Part 145 organizations implement an Information Security Management System (ISMS) to protect aviation safety from cybersecurity threats. This regulation, effective February 22, 2026, requires organizations to identify, assess, and mitigate information security risks related to maintenance activities.
- Key obligations include:
    - Risk Management (IS.I.OR.205 & IS.I.OR.210) – Organizations must systematically analyze cybersecurity risks.
    - Incident Reporting (IS.I.OR.215 & IS.I.OR.230) – Cyber incidents must be reported internally and externally within 72 hours of detection.
    - Personnel Training (IS.I.OR.240) – Cybersecurity training is mandatory for staff involved in maintenance operations.
    - Supply Chain Security (IS.I.OR.235) – Organizations must ensure third-party vendors meet cybersecurity standards.
- This regulation aligns with ISO 27001, ensuring organizations establish controls to prevent, detect, and respond to cyber threats while maintaining regulatory compliance.

2. What are the key differences between EASA's Information Security requirements under Part 145 and ICAO Annex 17, Security 4.9?

- ICAO Annex 17 focuses on aviation security (AVSEC) from an international perspective, while EASA's Part 145 information security regulations under (EU) 2023/203 are specifically targeted at aircraft maintenance organizations.
- Annex 17, 4.9.1 mandates that contracting states require operators to identify critical ICT systems and implement protection measures.
- EASA Part 145 (IS.I.OR.200 & IS.I.OR.205) expands this requirement, ensuring structured risk assessments, reporting, and continuous improvement.
- Annex 17 emphasizes supply chain security, while EASA's Part 145 mandates third-party vendor compliance (IS.I.OR.235).
- The key difference is that ICAO provides high-level guidance, while EASA regulations define detailed, enforceable compliance mechanisms for

maintenance organizations, ensuring cybersecurity measures are integrated within SMS.

3. How does the implementation of an Information Security Management System (ISMS) align with existing Part 145 SMS requirements?

- EASA mandates that ISMS be integrated into the existing Safety Management System (SMS) to ensure a holistic approach to risk management.
- SMS (EASA Part 145.A.200) manages operational risks; ISMS expands this by managing cybersecurity threats affecting aviation safety.
- Risk Assessment (IS.I.OR.205) – Cyber risks must be included in hazard identification and mitigation strategies.
- Incident Response (IS.I.OR.220) – ISMS requires cybersecurity incident procedures, complementing SMS safety reporting mechanisms.
- Compliance Audits (IS.I.OR.225) – Cybersecurity audits must align with SMS safety audits, ensuring a unified oversight process.
- By integrating ISMS into SMS, Part 145 organizations can prevent redundancy, optimize risk management, and meet regulatory obligations efficiently.

4. What are the major challenges that Part 145 organizations face in complying with cybersecurity regulations before the 2026 deadline?

- Key challenges include :
    - Limited Expertise: Many maintenance organizations lack dedicated cybersecurity personnel.
    - Budget Constraints: Cybersecurity investments, including training, tools, and compliance audits, require financial resources.
    - Legacy Systems: Older IT infrastructure may lack compatibility with modern cybersecurity controls.
    - Supply Chain Risks: Third-party compliance (IS.I.OR.235) is difficult to enforce across multiple vendors.
    - Cultural Resistance: Staff may resist new cybersecurity policies due to operational disruptions.
- To address these challenges, organizations should conduct a gap analysis (IS.I.OR.200), ensure cybersecurity training (IS.I.OR.240), and implement progressive ISMS improvements before full compliance is required in 2026.

5. How does the NIS2 Directive (EU) 2022/2555 influence cybersecurity management in EASA Part 145 organizations?

- The NIS2 Directive strengthens cybersecurity resilience for critical infrastructure, including aviation. It complements Regulation (EU) 2023/203 by:
    - Expanding Scope – Applies to all aviation entities managing critical ICT infrastructure.
    - Incident Reporting (72 hours rule) – Aligns with EASA's IS.I.OR.230 to ensure timely reporting.
    - Supply Chain Security – Enforces third-party risk management (IS.I.OR.235) and vendor cybersecurity standards.
    - Regulatory Enforcement – Competent authorities have stronger supervisory and penalty mechanisms for non-compliance.
- For Part 145 organizations, compliance with NIS2 ensures harmonization with broader EU cybersecurity policies, avoiding regulatory conflicts.

6. What are the most critical cyber threats faced by aircraft maintenance organizations today?

- Answer: Key threats include:
    - Ransomware Attacks: Targeting maintenance management systems, causing data encryption and operational disruptions.
    - Phishing Attacks: Social engineering exploits leading to unauthorized access.
    - Supply Chain Vulnerabilities: Weak security among third-party vendors (IS.I.OR.235).
    - Insider Threats: Employees misusing access to compromise systems.
    - Data Integrity Attacks: Manipulation of maintenance records, calibration data, or aircraft diagnostics.
- To counteract these threats, organizations must adopt multi-factor authentication (MFA), real-time monitoring, and continuous security training (IS.I.OR.240).

7. How do cyberattacks, such as ransomware or phishing, pose a risk to the safety of aircraft maintenance operations?

- Cyberattacks can directly impact airworthiness and operational safety:
    - Ransomware – Encrypts critical maintenance records, delaying aircraft release.
    - Phishing – Compromises access to technical databases, leading to unauthorized modifications.
    - Data Manipulation – False maintenance entries can result in undetected defects.

- IT System Disruptions – Interruptions in diagnostic software can lead to incorrect troubleshooting.
- Mitigation measures include network segmentation, MFA, and security awareness programs (IS.I.OR.240).

8. What risk assessment methodologies are recommended by EASA for evaluating cybersecurity risks in maintenance environments?

- EASA prescribes a structured risk assessment approach (IS.I.OR.205 & IS.I.OR.210), including:
  - ISO 27005 Risk Management Framework – Used to classify and prioritize cyber threats.
  - 5x5 Risk Matrix – Evaluates likelihood vs. severity of cybersecurity incidents.
  - Fault Tree Analysis (FTA) – Identifies failure pathways in critical systems.
  - Penetration Testing – Simulates cyberattacks to evaluate defenses.
  - Organizations should integrate these methods into their ISMS risk assessment process (IS.I.OR.200).

9. How should a Part 145 organization prioritize cybersecurity risks using structured risk assessment techniques?

- Risk prioritization under IS.I.OR.205 should follow these steps:
  - Identify Critical Assets – IT systems handling maintenance data, aircraft diagnostics, and regulatory compliance.
  - Assess Threat Likelihood & Impact – Using risk matrices and past incident data.
  - Apply Mitigation Measures – Implement firewalls, encryption, and endpoint security for high-risk areas.
  - Conduct Regular Audits – Periodic risk reviews to update controls.
  - This ensures resources are focused on mitigating the highest-impact threats first.
- A structured Security Risk Assessment (SRA) is essential for managing cybersecurity threats in EASA Part 145 organizations. The SRA process aligns with EASA IS.OR.205(b) and IS.OR.210(b) and involves four key phases:
- Risk Identification:
  - Identifying cybersecurity risks in the aircraft maintenance ecosystem.

  - Key areas of concern include MRO software vulnerabilities, digital data transmission security, remote access risks, insider threats, and emerging AI-driven cyber threats
- Risk Assessment:
- Using a Cybersecurity Risk Matrix to assess risks based on likelihood (rare to almost certain) and impact (negligible to severe).
- Example risks:
  - Unauthorized access to MRO software leading to falsified maintenance records.
  - Ransomware attacks disrupting scheduled maintenance operations.
  - Supply chain cyber breaches introducing malware

- **Risk Treatment:**
  - Implement mitigation strategies such as network segmentation, encryption, multi-factor authentication (MFA), and continuous monitoring.

- **Regulatory Compliance**: Align with EASA IS.OR.205(b) for risk identification and IS.OR.210(b) for risk management

10. What is the Role of Supply Chain Security in Mitigating Cyber Threats

- Supply chain security plays a vital role in reducing cyber risks in maintenance organizations by:
  - Evaluating Third-Party Vendors: Ensure suppliers comply with cybersecurity standards like ISO 27001.
  - Contractual Cybersecurity Clauses: Include clauses requiring secure development practices, vulnerability disclosure, and compliance audits.
  - Supplier Vetting & Audits: Regular security audits of suppliers to identify potential vulnerabilities.
  - Secure Data Sharing: Implement encrypted communication protocols and secure data exchange mechanisms between the organization and its vendors.

11 What are the Incident Response and Reporting Obligations

- Internal and External Reporting Obligations Under IS.I.OR.230 and IS.I.OR.215
- IS.I.OR.215 (Internal Reporting):
  - Establish an internal Incident Management System (IMS).
  - Report cybersecurity incidents to Information Security Officers (ISO).

    - Conduct impact assessments before escalating the report externally.
- IS.I.OR.230 (External Reporting):
    - Notify national aviation authorities of significant cyber incidents within 72 hours.
- Provide a follow-up report within 30 days, detailing:
    - Root cause analysis.
    - Mitigation actions taken.
    - Preventive measures implemented

.

12. What are the Key Steps in a Part 145 Organization's Cybersecurity Incident Response Plan

- Incident Detection & Classification (Identify attack vector, severity, and impacted systems).
- Initial Containment & Response (Isolate affected systems and prevent further spread).
- Impact Assessment & Notification (Evaluate risk to safety, compliance, and operations).
- Corrective & Preventive Actions (Implement recovery protocols and update security controls).
- Regulatory Reporting (Submit reports to EASA and national authorities as per IS.I.OR.230).
- Handling a Data Breach Involving Maintenance Records
- Immediate Containment: Disconnect compromised systems.
- Forensic Investigation: Determine scope and entry point of the breach.
- Data Integrity Checks: Verify if records were altered, deleted, or exfiltrated.
- Regulatory Reporting: Notify competent authorities under IS.I.OR.230(c).
- System Restoration: Restore data using encrypted backups.

12. What Information should be Included in an External Cybersecurity Incident Report

- Nature of the Incident (Malware, Data Breach, Ransomware, etc.).
- Affected Systems & Data.
- Potential Safety Impacts.
- Containment Measures Taken.
- Mitigation Actions & Recovery Plan.

- Recommendations for Future Prevention
- Ensuring Compliance with EASA's 72-Hour Cybersecurity Incident Reporting Requirement
- Implement an Automated Incident Detection System (AIDS).
- Train staff on reporting mechanisms and escalation.
- Maintain predefined templates for rapid incident reporting.
- Assign dedicated Information Security Officers to handle compliance.

13. What are the Typical Technical and Operational Cybersecurity Controls

- Minimum Technical Controls Required to Protect IT Systems in Maintenance Environments:
    - Firewall Protection: Enforce intrusion prevention systems (IPS).
    - Data Encryption: Secure stored and transmitted data.
    - Multi-Factor Authentication (MFA): Prevent unauthorized system access.
    - Regular Patch Management: Update systems to fix vulnerabilities.
    - Backup & Disaster Recovery: Implement offline, encrypted backups.
    - Best Practices for Securing Remote Access to Maintenance and Operational Systems
    - Zero Trust Architecture (ZTA): Validate every access request.
    - Virtual Private Networks (VPNs): Encrypt remote connections.
    - Role-Based Access Controls (RBAC): Restrict access based on job function.
    - Session Timeouts & Auto-Logout: Reduce exposure from unattended sessions.
    - Real-Time Monitoring & Logging: Detect unauthorized remote access attempts.

14. Discuss Enhancing Cybersecurity with Multi-Factor Authentication (MFA)

- MFA significantly enhances cybersecurity in Part 145 environments by requiring users to verify their identity using multiple authentication methods.
- Best practices for implementing MFA in MRO facilities include:
    - Biometric Authentication: Using fingerprint or facial recognition for access to critical maintenance systems.
    - Token-Based Authentication: Hardware security tokens or OTP (One-Time Password) applications to verify user access.
    - Behavioral Biometrics: Monitoring keystroke dynamics and mouse movement for additional verification.

- Role-Based Access: Implementing least privilege principles to ensure access is granted based on user role

15. How to Protect Maintenance Diagnostic Software from Cyber Manipulation

- Maintenance diagnostic software is vulnerable to cyberattacks, including malware injection, unauthorized data modification, and remote access threats. Mitigation strategies include:
  - Regular Patch Updates: Ensure all software is updated with the latest security patches.
  - Secure Sandboxing: Isolate diagnostic tools to prevent unauthorized network access.
  - Access Controls & MFA: Require multi-factor authentication before executing maintenance software commands.
  - Data Integrity Checks: Implement hash validation mechanisms to detect tampered data.
  - Redundancy Protocols: Use backup systems to override compromised diagnostic functions

16. Role of Network Segmentation in Mitigating Cybersecurity Risks

- Network segmentation enhances security by isolating critical maintenance systems from broader IT networks. Key benefits include:
  - Limited Attack Surface: Separates operational technology (OT) from IT networks to reduce exposure to external threats.
  - Micro-Segmentation: Restricts access within the network based on role and function.
  - Enhanced Monitoring: Improves anomaly detection by limiting movement of potential malware within segmented networks.
  - Regulatory Compliance: Aligns with EASA IS.OR.205(b) requirements for cybersecurity risk identification and management

17. Integration of ISO 27001 with EASA Cybersecurity Requirements

- ISO/IEC 27001 provides a framework for Information Security Management Systems (ISMS), which aligns with EASA Part 145 cybersecurity regulations. Integration includes:
  - Risk-Based Approach: ISO 27001 supports risk identification, assessment, and mitigation, aligning with EASA's IS.I.OR.205(b).

- Incident Response Framework: Facilitates structured reporting processes as required under IS.I.OR.230.
- Continuous Monitoring: Implements real-time security event logging to comply with EASA information security mandates

18. Discuss the Differences Between ISO/IEC 27001 and ISO/IEC 27005 in Aviation Cybersecurity

ISO/IEC 27001 establishes a framework for an Information Security Management System (ISMS), setting security controls and risk management practices to protect sensitive aviation data. Compliance ensures structured security governance against cyber threats.

ISO/IEC 27005 focuses on risk management within this framework, offering guidance on identifying and addressing cybersecurity risks. It aids aviation organizations in evaluating threats like cyber-attacks and unauthorized access. While ISO/IEC 27001 defines security measures, ISO/IEC 27005 provides a structured risk analysis methodology. Together, they enhance cybersecurity resilience in aviation.

19.What Lessons can be learnt from Industry-Wide Cybersecurity Incidents

- Part 145 organizations can enhance compliance and security posture by studying major cybersecurity incidents:
  - Ransomware Attacks (e.g., Colonial Pipeline): Highlight the importance of network segmentation and backups.
  - SolarWinds Supply Chain Attack: Demonstrates the need for third-party security audits.
  - Boeing Data Breach: Emphasizes data encryption and strict access control.
- Lessons Learned:
  - Implement Zero Trust Architecture (ZTA).
  - Strengthen supply chain security.
  - Establish automated anomaly detection systems

20. How to achieve Continuous Improvement in Cybersecurity Risk Management

- Regular Cyber Drills: Simulate ransomware and phishing attacks for personnel training.
- Automated Threat Detection: Use AI-based monitoring tools for proactive risk mitigation.

- Periodic ISO 27001 Audits: Conduct gap analyses and compliance checks.
- Lessons from Cyber Incidents: Incorporate findings from EASA & ICAO security reports into security policies

21. How to Conduct a ISO 27001 Gap Analysis?

- Step 1: Map current cybersecurity policies to ISO 27001 requirements.
- Step 2: Identify compliance gaps in access controls, encryption, and incident response.
- Step 3: Conduct internal audits and penetration testing.
- Step 4: Implement corrective actions and conduct follow-up assessments

22. What Cybersecurity Training is required for Maintenance Personnel?

- Basic Cyber Hygiene: Password security, email phishing awareness.
- Incident Response Protocols: How to report and respond to cybersecurity threats.
- System Access Best Practices: Secure login procedures with MFA.
- Practical Drills: Hands-on training with simulated cyber incidents

23. How to Overcome Cultural Resistance to Cybersecurity Compliance

- Executive Buy-In: Top-down security culture enforcement.
- Gamification & Incentives: Reward employees for identifying cybersecurity threats.
- Clear Communication: Explain how cybersecurity impacts safety & operations

24. How to Improve Cybersecurity Awareness Among Subcontractors & Suppliers

- Mandatory Training Programs: Require third-party cybersecurity training.
- Security Clauses in Contracts: Enforce ISO 27001 compliance in vendor agreements.
- Regular Vendor Audits: Conduct penetration testing on supplier networks

25. Identify the evolution of the Compliance & Safety Manager's Role

- With ISMS implementation, the Compliance & Safety Manager must:
    - Oversee Cyber Risk Management: Ensure alignment with IS.I.OR.205(b).
    - Manage External Reporting Obligations: Handle 72-hour EASA cyber incident reports.

- Implement Continuous Cybersecurity Training: Ensure regulatory compliance and awareness

26. How to develop Key Performance Indicators (KPIs) for Cybersecurity Effectiveness

- KPI Measurement Criteria
  - Incident Detection Time
  - Speed of detecting cyber threats
  - Incident Response Time
  - Time taken to neutralize threats
  - Phishing Test Success Rate
  - Percentage of employees avoiding phishing attempts
  - Patch Compliance Rate
  - Percentage of systems updated on time
  - Third-Party Security Audit Results
  - Compliance levels with security standards