SOFEMA AVIATION SERVICES

Stakeholder Risk Information Sharing Requirements in Cybersecurity and Information Security within an EASA Part 145 Organization

Presented by Sofema Aviation Services (SAS)

Introduction

As aircraft maintenance operations become increasingly digitized, cybersecurity must be integrated into safety and operational risk management frameworks. Implementing a structured SRA process ensures that Part 145 organizations and stakeholders can proactively mitigate cyber threats, safeguard aircraft airworthiness, and comply with evolving regulations.

By identifying these interfaces and implementing cybersecurity best practices, organizations can minimize vulnerabilities, protect sensitive data, and ensure regulatory compliance.

- Effective risk information sharing is a fundamental component of cybersecurity and information security within an EASA Part 145 organization.
- The security risk assessment (SRA) process plays a vital role in mitigating cyber threats that could compromise aviation safety.
- Here we outline the obligations of key stakeholders—maintenance organizations, OEMs, software providers, and regulatory bodies—to assess, treat, and communicate cybersecurity risks.
- To also highlights best practices for implementing a structured approach to managing information security risks within the Part 145 maintenance environment.

Cybersecurity Risk Assessment (SRA) as a Core Process in Aircraft Maintenance Operations

Cybersecurity threats pose a growing challenge in aircraft maintenance, given the increasing reliance on digital systems, cloud-based MRO platforms, electronic logbooks, and interconnected operational environments.

- A Security Risk Assessment (SRA) is an essential structured approach for identifying, evaluating, and mitigating cybersecurity risks that may impact maintenance organizations, system suppliers, and the broader aviation ecosystem.

- SRA is not a one-time activity; it is a continuous process that adapts to evolving threats, regulatory requirements, and technological advancements. In the context of EASA Part 145 organizations, cybersecurity risk management aligns with EASA IS.OR.205(b) and IS.OR.210(b) to ensure the effective identification and mitigation of risks.

Core Components of the SRA Process

A structured SRA involves four key phases: Risk Identification, Risk Assessment, Risk Treatment, and Regulatory Compliance.

Risk Identification - The first step in SRA involves a systematic identification of cybersecurity risks within the aircraft maintenance ecosystem. Key considerations include:

- Digital Interfaces & MRO Software: Maintenance, Repair, and Overhaul (MRO) platforms, electronic maintenance records, and connected diagnostic tools introduce cybersecurity risks.
- Data Integrity & Transmission: Aircraft maintenance data is often transmitted via secure communication channels, and any breach can compromise operational reliability.
- Connected Supply Chain: Cybersecurity risks extend to system suppliers, OEMs, and third-party service providers.
- Remote Access & Cloud-Based Solutions: Increased reliance on remote troubleshooting and cloud-based systems requires robust access controls and encryption mechanisms.
- Insider Threats & Human Factors: Employees and contractors handling sensitive maintenance data could be potential cybersecurity risks.
- Emerging Threats (AI & Advanced Persistent Threats - APTs): The use of AI-driven attacks and nation-state threats targeting aviation infrastructure is a growing concern.

Risk Assessment - Once risks are identified, they must be assessed based on their likelihood and impact. This is typically done using a risk matrix that categorizes threats into different levels of severity:

Key Risk Metrics:

- Likelihood: Probability of occurrence (e.g., rare, unlikely, possible, likely, almost certain)
- Impact: Consequences on maintenance operations (e.g., negligible, minor, moderate, major, severe)
- Exposure & Vulnerability: How susceptible an organization is to cyber threats based on system architecture and existing defenses.

Example Risk Scenarios:

- Unauthorized Access to MRO Software: Could result in fraudulent modifications to maintenance records, affecting aircraft airworthiness.
- Ransomware Attack on a Maintenance Provider: Might encrypt critical maintenance data, delaying scheduled aircraft servicing.
- Supply Chain Cyber Breach: A supplier's compromised system could introduce malware into Part 145 organizations.

Risk Treatment

After identifying and assessing risks, mitigation strategies must be implemented. Best practices include:

Technical Controls:

- Network Segmentation & Firewalls: Restrict unauthorized access to critical maintenance data.
- Encryption & Secure Protocols: Ensure end-to-end encryption for all maintenance data transmissions.
- Multi-Factor Authentication (MFA): Secure access to MRO platforms and electronic records.
- Regular Patch Management & Updates: Mitigate vulnerabilities in software and IT systems.

Administrative & Operational Controls:

- Cybersecurity Training for Maintenance Personnel: Ensure all staff are aware of cyber threats and safe practices.

- Incident Response & Recovery Plans: Develop robust procedures for identifying, containing, and mitigating cyber incidents.
- Third-Party Risk Management: Conduct security audits for system suppliers and vendors.
- Access Control Policies: Implement least-privilege access to limit exposure.

Regulatory Compliance

Part 145 organizations must align their SRA approach with EASA IS.OR.205(b) and IS.OR.210(b) requirements:

- IS.OR.205(b) – Cybersecurity Risk Identification & Communication
  Requires organizations to systematically identify cybersecurity risks and communicate them with relevant stakeholders.
- IS.OR.210(b) – Cybersecurity Risk Management
  Mandates the management of shared cybersecurity risks across the maintenance ecosystem, requiring a collaborative approach among MROs, OEMs, suppliers, and aviation authorities.

Other relevant regulatory frameworks include:

- ICAO Aviation Cybersecurity Framework
- NIST Cybersecurity Framework
- EU NIS2 Directive (for critical aviation infrastructure security)

To enhance cybersecurity resilience, organizations should:

1. Perform regular SRA updates to adapt to new threats.
2. Invest in cybersecurity training for maintenance personnel.
3. Develop real-time monitoring capabilities to detect and respond to cyber incidents.
4. Strengthen collaboration with regulators and suppliers to share cybersecurity intelligence.

By embedding cybersecurity risk management into core aviation maintenance processes, organizations can achieve greater resilience, compliance, and operational integrity in an increasingly digital ecosystem.

Understanding Shared Interfaces and Cyber Exposure

Part 145 organizations operate within an interdependent digital ecosystem involving aircraft operators, OEMs, regulatory authorities, and third-party service providers. This connectivity, while improving operational efficiency, also introduces cybersecurity vulnerabilities. Shared interfaces act as potential entry points for cyber threats, making it crucial to identify and manage risks systematically.

Key Shared Interfaces in Part 145 Organizations

The digital infrastructure in maintenance, repair, and overhaul (MRO) is built on various interfaces that facilitate seamless data exchange and operational coordination. However, these connections also increase cybersecurity risks, including unauthorized access, malware infiltration, and data manipulation.

MRO Systems and Aircraft Connectivity

- Electronic Technical Records & Maintenance Logs: Digital platforms like Traxxall, Rusada ENVISION, and AMOS store and exchange aircraft maintenance data.
- Predictive Maintenance Platforms: AI-driven tools that monitor aircraft health, such as Airbus Skywise and Boeing AnalytX, require continuous data transmission.
- Onboard-to-Ground Communication Systems: Real-time aircraft health monitoring systems transmit operational data via SATCOM and ACARS, exposing Part 145 organizations to cyber threats from unsecured links.

MRO Systems and Aircraft Connectivity Cyber Risks:

- Data tampering, affecting airworthiness decisions.
- Malware or ransomware targeting technical record databases.
- Unsecured APIs allowing unauthorized data access.

OEM-Operator Digital Exchange

- Software Updates & Patches: Aircraft manufacturers such as Airbus and Boeing regularly release firmware and software updates for avionics, onboard systems, and maintenance applications.

- Data Sharing via Digital Platforms: OEMs provide maintenance service bulletins, part tracking, and reliability analysis through platforms like Airbus Airman and Boeing Toolbox.
- Supplier Integration: Third-party suppliers interact with Part 145 organizations via cloud-based services, increasing the attack surface.

OEM-Operator Digital Exchange Cyber Risks:

- Supply chain attacks where malicious updates are injected into critical software.
- Data interception in unencrypted communication channels.
- Phishing campaigns targeting maintenance personnel for unauthorized access.

Regulatory and Compliance Portals

- EASA Safety Reporting Systems (ECCAIRS 2, Safety Management System portals).
- National CAA Electronic Data Submission Platforms for compliance reporting.
- Aircraft Maintenance Data Exchange with Lessors & Auditors.

Regulatory and Compliance Portals Cyber Risks:

- Unauthorized access to regulatory submission portals, leading to data leaks.
- Malware-infected regulatory software that compromises connected systems.
- Data integrity risks where compliance reports could be altered or manipulated.

Best Practices for Managing Cyber Exposure

To mitigate these risks, Part 145 organizations must establish structured cybersecurity defenses through the following best practices:

Conduct Interface Mapping

- Identify and document all digital connections between internal systems, OEMs, operators, and regulators.
- Classify interfaces by sensitivity level (e.g., critical, high, medium, low) based on potential cyber impact.
- Assess access controls, encryption levels, and authentication mechanisms in shared digital platforms.

Develop a Common Framework

- Implement ISO 27001-based risk assessments to ensure cybersecurity policies align with industry best practices.
- Adopt the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) for continuous risk mitigation.
- Require third-party vendors (OEMs, IT providers, suppliers) to comply with cybersecurity standards.

Establish Continuous Monitoring

- Deploy Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) solutions to track suspicious activities.
- Implement real-time vulnerability scanning for early threat detection.
- Develop cyber incident response plans to handle data breaches and ransomware attacks swiftly.

Strengthen Access Controls & Authentication

- Enforce Multi-Factor Authentication (MFA) for all maintenance system logins.
- Restrict role-based access to minimize exposure to sensitive data.
- Implement zero-trust architecture, requiring verification for every access attempt.

Secure Data Transmission

- Use end-to-end encryption for data exchange with aircraft systems, OEMs, and regulators.
- Ensure compliance with EASA’s cybersecurity directives for safe data handling in aviation maintenance.
- Regularly update firewall rules and network segmentation to isolate critical systems from potential cyber threats.

Cybersecurity Information Sharing Between Connected Organizations

In the increasingly interconnected aviation ecosystem, cybersecurity threats can propagate rapidly across different stakeholders, including maintenance organizations, original equipment manufacturers (OEMs), software vendors, and regulators.

- Proactive information sharing is vital for managing cyber risks and minimizing the impact of cybersecurity incidents.
- Effective information sharing should be structured, secure, and integrated into cybersecurity risk management frameworks.

Best Practices for Cybersecurity Information Sharing

Cybersecurity information sharing between connected organizations is a cornerstone of modern cybersecurity risk management.

By adopting timely risk communication, standardized reporting mechanisms, and collaborative mitigation strategies, stakeholders can enhance threat detection, accelerate incident response, and improve industry-wide cybersecurity resilience.

Timely Risk Communication

Cyber threats evolve quickly, and delayed communication can increase an organization's exposure to risks. Maintenance organizations, OEMs, software vendors, and regulators must adopt established channels and protocols to ensure swift notification of emerging cyber threats.

Key Aspects:

- Real-Time Alerts: Use automated notification systems (e.g., SIEM tools, threat intelligence platforms) to disseminate real-time alerts.
- Secure Information Exchange: Utilize encrypted communication channels such as Aviation ISAC (Information Sharing and Analysis Centers), dedicated industry portals, and secure emails.
- Defined Response Teams: Designate cybersecurity response teams within each organization to handle threat communications.

Example: A cyber vulnerability detected in a widely used avionics software must be shared with all affected parties immediately. Delays could result in multiple airlines being compromised.

Standardized Reporting Mechanisms

The lack of uniformity in reporting cybersecurity threats and incidents can lead to misinterpretation or incomplete information dissemination. A structured and standardized approach ensures clarity and actionability.

Key Aspects:

- Unified Reporting Formats: Utilize industry-standard frameworks like STIX (Structured Threat Information eXpression) and TLP (Traffic Light Protocol) to categorize and share threat intelligence.
- Regulatory Compliance: Align reports with regulatory guidelines such as EASA's Cybersecurity Regulatory Framework, FAA's AC 119-1, and EU NIS Directive.
- Incident Categorization: Define severity levels (e.g., low, medium, high, critical) for cyber threats and incidents to prioritize responses.

Example: A malware attack on an aircraft maintenance database should be reported in a standardized format detailing its origin, impact, mitigation measures, and potential risks to other systems.

Collaborative Risk Mitigation

Proactive risk mitigation requires cross-industry collaboration to develop joint cybersecurity risk assessments and response plans.

Key Aspects:

- Cybersecurity Exercises & Simulations: Conduct joint cybersecurity drills between maintenance organizations, OEMs, and software vendors to test coordinated responses to cyber threats.
- Threat Intelligence Sharing Agreements: Establish partnerships through industry groups. like IATA's Aviation Cybersecurity Strategy.
- Supply Chain Cyber Risk Management: Ensure that cybersecurity measures extend to subcontractors and third-party vendors.

Example: An OEM collaborates with maintenance organizations and software vendors to test and patch a cybersecurity vulnerability found in aircraft maintenance software before attackers can exploit it.

Challenges in Cybersecurity Information Sharing

While information sharing is crucial, organizations often face challenges such as:

1. Legal and Compliance Barriers – Regulations like GDPR, CISA, and ITAR may restrict the sharing of cybersecurity-related data.
2. Lack of Trust – Competing entities may hesitate to share critical cyber threat data due to reputational risks or competitive concerns.

3. Data Sensitivity – Cybersecurity incidents often involve sensitive operational and financial information.
4. Standardization Issues – Organizations may follow different cybersecurity protocols, leading to compatibility issues in threat intelligence sharing.

For aviation organizations, participating in industry-wide cybersecurity alliances and implementing robust information-sharing protocols can significantly reduce the likelihood and impact of cyber threats while fostering a safer digital ecosystem.

Continuous Cyber Risk Assessment and Update Mechanisms for EASA Part 145 Organizations

Cybersecurity threats are constantly evolving, posing significant risks to aviation maintenance organizations operating under EASA Part 145. The introduction of EASA IS.OR.205(d2) mandates that organizations regularly review and update risk assessments when security conditions change. To maintain compliance and ensure a robust security posture, organizations must establish continuous cyber risk assessment mechanisms and implement proactive update strategies.

Regulatory Framework – EASA IS.OR.205(d2)

EASA requires that Part 145 organizations integrate cybersecurity measures into their Safety Management Systems (SMS). Specifically, IS.OR.205(d2) mandates that organizations:

- Regularly review cybersecurity risks in line with changing security conditions.
- Update risk assessments whenever new threats or vulnerabilities are identified.
- Establish mitigation strategies that align with evolving cyber risks.

This regulation reinforces the need for a structured and proactive cybersecurity risk management approach.

Best Practices for Continuous Cyber Risk Assessment

A well-defined cyber risk management framework ensures that Part 145 organizations can identify, assess, and mitigate threats effectively. Best practices include:

Periodic Review Cycles

- Implement a structured review process at predefined intervals (e.g., quarterly, semi-annually, or annually).
- Align these reviews with broader safety audits, compliance checks, and SMS reviews.
- Utilize a Cybersecurity Risk Matrix to prioritize threats based on likelihood and impact.
- Conduct vulnerability assessments and penetration testing at regular intervals to detect potential weaknesses.

Incident-Driven Updates

- Incorporate a dynamic update mechanism that ensures risk assessments are reviewed immediately after:
    - A cyber incident (e.g., data breach, malware attack, or phishing attempt).
    - A change in the organization's IT infrastructure or security policies.
    - New cybersecurity threats or intelligence reports from industry sources (e.g., EASA, ICAO, ENISA, or CERT).
- Update security policies to include new mitigation controls, such as patching vulnerabilities, access control enhancements, or improved network monitoring.

Training and Awareness Programs

- Conduct regular cybersecurity training for maintenance personnel, engineers, and IT staff to:
    - Identify social engineering attacks (e.g., phishing, insider threats).
    - Recognize and report cyber anomalies.
    - Understand cybersecurity best practices specific to aviation maintenance.
- Utilize simulated phishing campaigns to assess employee awareness.
- Develop incident response drills to improve response times and decision-making during cybersecurity events.

Implementing an Adaptive Cyber Risk Management Approach

To ensure that cybersecurity defenses remain effective, organizations must implement a continuous improvement cycle that includes:

Risk Identification and Threat Intelligence

- Use threat intelligence sources (e.g., EASA alerts, Aviation ISAC, industry reports) to stay informed about emerging risks.
- Perform cyber risk mapping to identify potential vulnerabilities in aircraft maintenance software, supply chain networks, and IoT-connected devices.

Continuous Monitoring and Detection

- Deploy Security Information and Event Management (SIEM) systems to detect anomalies.
- Utilize Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for proactive defense.
- Implement endpoint protection to safeguard maintenance laptops, tablets, and mobile devices used in Part 145 environments.

Automated Response and Recovery Mechanisms

- Establish automated threat detection and response protocols.
- Develop cyber incident playbooks to standardize response procedures.
- Implement regular backups and disaster recovery plans to minimize downtime in case of cyber incidents.

Conclusion - Continuous cyber risk assessment is a regulatory requirement under EASA IS.OR.205(d2) and a critical component of a robust cybersecurity strategy for Part 145 organizations.

By implementing –

- Periodic review cycles
- Incident-driven updates
- Ongoing training and
- Awareness Threat intelligence monitoring
- Automated response mechanisms

Part 145 organizations can stay ahead of evolving cyber threats, enhance operational resilience, and maintain compliance with EASA cybersecurity regulations.

5. Compliance and Industry Standards Alignment

To ensure a structured and effective approach to cybersecurity risk information sharing, Part 145 organizations should align their practices with industry standards and regulatory requirements, including:

- **EASA Regulations** (e.g., IS.OR.205 and IS.OR.210)
- **ICAO Annex 17 – Aviation Security (Cybersecurity Aspects)**
- **ISO 27001 – Information Security Management**
- **NIST Cybersecurity Framework for risk management**
- **EU NIS 2 Directive for Aviation Cybersecurity Compliance**

Best Practices:

- **Maintain Compliance Documentation:** Keep detailed records of cybersecurity risk assessments, incidents, and mitigation measures.
- **Regular Audits and Assessments:** Conduct internal and external cybersecurity audits to verify compliance with regulatory and industry standards.
- **Leverage Industry Collaboration:** Participate in aviation cybersecurity working groups to share best practices and threat intelligence.

Summary

Risk information sharing is a fundamental pillar of cybersecurity and information security within an EASA Part 145 organization. Ensuring that cyber threats are not isolated but collectively addressed strengthens the resilience of aviation maintenance operations. By implementing structured Security Risk Assessments (SRA), identifying shared interfaces, communicating cybersecurity risks, continuously updating risk assessments, and aligning with industry standards, Part 145 organizations can establish a robust framework for managing information security threats.

The key takeaway is that cybersecurity is a shared responsibility—proactive collaboration and transparency among maintenance providers, OEMs, software

vendors, and regulatory authorities are essential for ensuring the safety and resilience of aviation maintenance systems.

Next steps – please see the following - https://sassofia.com/news-press/a-new-training-dedicated-to-implementing-an-information-cyber-security-program-in-an-easa-part-145-organization-is-now-available-book-your-place/

Visit www.sassofia.com or email office@sassofia.com