REVISION LOG

Update notices for this book will be available online at www.actechbooks.com/revisions.html
If you would like to be notified when changes occur, please join our mailing list at www.actechbooks.com

VERSION	EFFECTIVE DATE	DESCRIPTION OF REVISION(S)
001	2014.02	Module creation and release.
002	2017.05	Format Update/Addition of Part-T, Submodule 6.
003	2019.08	Updated to current regulations, and reduction of Submodule 4 to appropriate level 1 requirements.
004	2020.10	Enhanced or modified content within the following Submodules: Submodule 1: Updated to current regulations EU 2018/1139 and 376/2014 Submodule 2: Definitions section added Submodule 3: Definitions section added Submodule 4: Complete rewrite for updated regulations Submodule 5: Definitions section added Submodule 6: Complete rewrite for updated regulations Submodule 7: Definitions section added
004.1	2021.04	Submodule 3: Corrected answer to question 3-2 from 2 to 3.
004.2	2023.04	Inclusion of Measurement Standards for clarification, page iv. Minor appearance and format updates.
005	2024.04	Regulatory update for EASA 2023-989 compliance.
005.1	2024.06	Submodule 5: Self-declaration Authorizations - topic added.
005.2	2025.01	Form 2-2, A and B added (EASA Form 19).
005.3	2025.05	Complete rewrite of Submodule 10, improved and removed figures throughout.

Module was reorganized based upon the EASA 2023-989 subject criteria. Enhancements included in this version 005.3 are:

10.1 *Regulatory Framework* - Added the relationship between regulations (hard law) and AMC, GM and CSS (soft law).
10.1 *Regulatory Framework* - Added occurrence reporting EU 376/2014.
10.1 *Regulatory Framework* - Added relationship between the annexes.
10.3 *Approved Maintenance Organisations* - Added Combined Airworthiness Organizations
10.5 *Air Operations* - Added topic.
10.4 *Independent Certifying Staff* - Added new content.
10.9 *Maintenance and Certification Beyond Current EU Regulations* - Added description of EMAR regulations.
10.10 *Cybersecurity in Aviation Maintenance* - Complete rewrite.
Replaced all questions and answers.

Cybersecurity in Aviation Maintenance

Submodule 10

SUBMODULE KNOWLEDGE DESCRIPTIONS		LEVEL
		B1/B2
10.10	**Cybersecurity in Aviation Maintenance** Regulation on the introduction of organisation requirements for the management of information security risks related to aeronautical information systems used in civil aviation.	1

10.10 - CYBERSECURITY IN AVIATION MAINTENANCE

CYBERSECURITY IN AVIATION MAINTENANCE

The aerospace industry has increasingly become a prime target for cyberattacks, primarily because of its dependence on highly interconnected digital systems, extensive global supply chains, and the substantial amount of sensitive information it processes. The Maintenance, Repair, and Overhaul (MRO) sector is particularly vulnerable to cyber threats for several reasons. MROs have access to major airlines as well as manufacturers of engines and components. Although MROs may not be the direct target of cybercriminals, they can serve as a gateway for attacks on the aircraft.

SECURING AERONAUTICAL INFORMATION SYSTEMS

The aviation sector has experienced a digital transformation over the last 15 to 20 years, encompassing everything from airline operations to aircraft, ground systems, and their interconnected networks. With the implementation of these digital systems and advanced technologies, the industry must adopt essential cybersecurity measures to maintain safety, reliability, and resilience.

The primary objective of aviation cybersecurity is to safeguard aircraft and their associated systems from potential cyber threats. This involves protecting the safety and integrity of communication, navigation, and operational systems onboard the aircraft.

Cybersecurity plays a crucial role in ensuring that data transmitted from an aircraft to organizational networks remains secure, thereby preventing unauthorized access and information theft. Continuous risk mitigation is a fundamental aspect of cybersecurity efforts.

TYPES OF CYBER-ATTACKS

Aviation Maintenance, Repair, and Overhaul (MRO) organizations role is critical for the safety and efficiency of aircraft operations. MRO organizations face a range of cyber threats, including ransomware, phishing, data breaches, exploitation of IT vulnerabilities, insider threats, and DDoS attacks. Understanding the most common types of cyber threats can help implement effective defenses.

RANSOMWARE ATTACKS

Ransomware is one of the most significant threats to MRO organizations. In these attacks, cybercriminals encrypt critical data and demand a ransom for its release. Ransomware can disrupt maintenance schedules, compromise sensitive information, and lead to substantial financial losses. The aviation sector has seen a sharp increase in ransomware incidents, with attackers often targeting the interconnected systems used in aircraft maintenance.

PHISHING ATTACKS

Phishing attacks involve tricking individuals into providing sensitive information, such as login credentials or financial details, by posing as a trustworthy entity. MRO staff are often targeted through emails that appear to be from legitimate sources. Successful phishing attacks can lead to unauthorized access to systems, data breaches, and financial fraud.

DATA BREACHES

Data breaches occur when cybercriminals gain unauthorized access to sensitive information. In the context of MRO organizations, this can include maintenance records, operational data, and personal information of employees. Data breaches can result in the theft of intellectual property, regulatory fines, and damage to the organization's reputation.

EXPLOITATION OF IT VULNERABILITIES

Cybercriminals often exploit vulnerabilities in software and hardware to gain access to systems. These vulnerabilities can exist in operating systems, applications, or even the interconnected devices used in aircraft maintenance. Exploiting these weaknesses can allow attackers to disrupt operations, steal data, or manipulate maintenance processes.

INSIDER THREATS

Insider threats involve malicious actions taken by employees or individuals with access to the organization's systems. These threats can be intentional, such as sabotage, data theft, or unintentional, such as accidental disclosure of sensitive information. Insider threats are particularly challenging to detect and mitigate.

DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

DDoS attacks aim to overwhelm an organization's network by flooding it with excessive traffic, causing disruptions to services. For MRO organizations, DDoS attacks can hinder access to critical systems and delay maintenance operations. These attacks can be particularly damaging if they target systems that manage aircraft schedules and maintenance records

PREVENTING CYBERATTACKS

MRO organizations must implement a comprehensive set of cybersecurity measures to protect their operations and data. By adopting network segmentation, regular software updates, employee training, IDPS, data encryption, security audits, incident response plans, they can significantly enhance their cybersecurity defenses.

NETWORK SEGMENTATION AND ACCESS CONTROL

One of the fundamental cybersecurity measures is network segmentation. By dividing the network into smaller, isolated segments, MRO organizations can limit the spread of cyberattacks. Access control mechanisms should be implemented to ensure that only authorized personnel have access to specific segments of the network. This reduces the risk of unauthorized access to critical systems and sensitive data.

REGULAR SOFTWARE UPDATES AND PATCH MANAGEMENT

Keeping software and systems up to date is crucial in defending against cyber threats. MRO organizations should establish a robust patch management process to ensure that all software, including operating systems and applications, are regularly updated with the latest security patches. This helps to close vulnerabilities that cybercriminals could exploit.

EMPLOYEE TRAINING AND AWARENESS PROGRAMS

Human error is often a significant factor in cybersecurity breaches. MRO organizations should invest in comprehensive training and awareness programs for their employees. These programs should educate staff about common cyber threats, such as phishing and social engineering, and provide guidelines on how to recognize and respond to these threats. Regular training sessions can help create a culture of cybersecurity awareness within the organization.

IMPLEMENTATION OF INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)

Intrusion Detection and Prevention Systems (IDPS) are essential tools for monitoring network traffic and identifying potential cyber threats. By implementing IDPS, MRO organizations can detect and respond to suspicious activities in real-time, preventing cyberattacks before they cause significant damage. These systems can also provide valuable insights into the nature of the threats, helping to improve overall cybersecurity strategies.

DATA ENCRYPTION

Encryption plays a strong role in cybersecurity, and is vital to ensure the integrity and confidentiality of data within aircraft systems. Encryption plays a key role in digital signatures that the industry relies on for maintenance and configuration control such as ensuring that software parts have not been modified, that LRUs are correctly adopted by the aircraft, and that PDLs are correctly authenticated. Many aircraft systems currently lack adequate encryption, exposing them to potential cyber threats.

SECURE COMMUNICATION

Secure communication protocols, such as HTTPS and VPNs, should be used to protect data transmitted over the internet. This helps to safeguard maintenance records, operational data, and other sensitive information from cyber threats.

REGULAR SECURITY AUDITS AND VULNERABILITY ASSESSMENTS

Conducting regular security audits and vulnerability assessments is essential to identify and address potential weaknesses in the cybersecurity infrastructure. MRO organizations should perform these assessments periodically to ensure that their systems and processes are secure. External audits by third-party cybersecurity experts can provide an unbiased evaluation of the organization's security posture and recommend improvements.

INCIDENT RESPONSE AND RECOVERY PLANS

Having a well-defined incident response and recovery plan is crucial for minimizing the impact of cyberattacks. MRO organizations should develop and regularly update their incident response plans to ensure a swift and effective response to cybersecurity incidents. These plans should include procedures for identifying, containing, and mitigating cyber threats, as well as steps for recovering affected systems and data.

PERSONAL PROTECTION AGAINST CYBERATTACKS

Personal protection against cyberattacks involves a combination of strong passwords, multifactor authentication, regular software updates, cautious email and internet practices, data backups, and ongoing education. By adopting these practices, individuals can significantly reduce risk of cyberattacks in their organization.

STRONG PASSWORDS AND MULTIFACTOR AUTHENTICATION

One of the fundamental steps in protecting oneself from cyberattacks is the use of strong, unique passwords. A strong password typically includes a combination of letters (both uppercase and lowercase), numbers, and special characters. Using a password manager can help generate and store complex passwords securely. Additionally, enabling multifactor authentication (MFA) adds an extra layer of security. MFA requires not only a password but also a second form of verification, such as a code sent to your phone, making it significantly harder for attackers to gain access.

REGULAR SOFTWARE UPDATES

Keeping software up to date is another critical aspect of cybersecurity. Software updates often include patches for security vulnerabilities that cybercriminals can exploit. Regularly updating your operating system, applications, and antivirus software ensures that you have the latest protections against known threats.

EMAIL AND INTERNET CAUTION

Phishing attacks, where attackers trick individuals into providing sensitive information, are common. Being cautious with emails and avoiding clicking on links or downloading attachments from unknown or suspicious sources can prevent many cyberattacks. Similarly, using secure networks and avoiding public Wi-Fi for sensitive transactions can protect against data interception. When necessary, using a Virtual Private Network (VPN) can encrypt your internet connection, adding an additional layer of security.

DATA BACKUP

Regularly backing up important data is a crucial step in mitigating the impact of ransomware attacks, where attackers lock your data and demand payment for its release. By keeping backups on external drives or cloud services, you can restore your data without having to pay the ransom.

EDUCATION AND AWARENESS

Staying informed about the latest cyber threats and learning how to recognize and respond to them is vital. Cybersecurity is an ever-evolving field, and new threats emerge regularly. By educating yourself and staying aware of current trends, you can better protect yourself against potential attacks.

AVIATION CYBERSECURITY REGULATIONS AND STANDARDS

Both EASA and the FAA have issued new regulations that mandate proactive assessment and mitigation of potential cyber vulnerabilities in aviation. These regulations are designed to ensure that airlines and other aviation stakeholders take necessary steps to protect aircraft and associated systems from cyber threats.

FEDERAL AVIATION ADMINISTRATION (FAA)

The current trend in airplane design includes an increasing level of integration of airplane, engine, and propeller systems with increased connectivity to internal or external data networks and services. Regulators and industry must constantly monitor the cybersecurity threat environment in order to identify and mitigate new threat sources. These designs can introduce or allow cybersecurity vulnerabilities from sources such as:

- Field Loadable Software;
- Maintenance laptops;
- Airport or airline gate link networks;
- Public networks, e.g., internet;
- Wireless aircraft sensors and sensor networks;
- Cellular networks;
- Universal Serial Bus (USB) devices;
- Satellite communications;
- Portable electronic devices and portable electronic flight bags (EFBs); and
- GPS and satellite-based augmentation system digital data.

The FAA has found that its current airworthiness regulations are inadequate and inappropriate to address the cybersecurity vulnerabilities caused by increased interconnectivity.

In 2024, the FAA proposed to add new regulations and revise certain existing regulations in title 14, Code of Federal Regulations (14 CFR) part 25 (Airworthiness Standards: Transport Category Airplanes), part 33 (Airworthiness Standards: Aircraft Engines), and part 35 (Airworthiness Standards: Propellers). This proposed rulemaking imposes new design standards to address cybersecurity threats for transport category airplanes, engines, and propellers.

These changes introduce type certification and continued airworthiness requirements to protect the equipment, systems and networks of transport category airplanes, engines and propellers against intentional unauthorized electronic interactions (IUEI) that could create safety hazards. Design approval applicants would be required to identify, assess and mitigate such hazards, and develop Instructions for Continued Airworthiness (ICA) that would ensure such protections continue in service. Proposed changes to parts 25, 33, and 35 mandate such protection and apply to applicants for design approval of transport category airplanes, engines and propellers.

EASA/EU REGULATION

The introduction of EASA Part-IS (Information Security), aligned with Regulation (EU) 2023/203, establishes mandatory cybersecurity requirements to safeguard aviation organizations, including Continuing Airworthiness Management Organizations (CAMOs) and, Part-145 maintenance organizations, along with other stakeholders.

EASA REGULATIONS PART IS

Part-IS compliance involves aligning EASA's cybersecurity framework with existing aviation safety regulations such as Part-145, Part-CAMO, and SMS requirements. [**Figure 10-1**]

Figure 10-1. EASA Easy Access Rules for Part-IS.

The regulation applies to several organizations, including:

- Part-145 Maintenance Organizations (excluding certain smaller entities).
- Continuing Airworthiness Management Organizations (CAMOs).
- Approved Training Organizations (ATOs) and Air Navigation Service Providers (ANSPs), among others.
- Organizations that consider Part-IS is not applicable/ outside its scope can request derogations under specific provisions.
- EASA Regulations Part IS require airlines to address cybersecurity comprehensively and start proactively monitoring and mitigating cyber threat. This regulation has significant implications for MRO organizations, which must satisfy following requirements:
- Information Security Management: MRO organizations must implement robust information security management systems to protect their ICT systems and data used in aviation. This includes identifying and managing information security risks.
- Incident Response: MROs are required to have procedures in place for detecting, responding to, and recovering from information security incidents. This ensures that any disruptions to maintenance operations are minimized and aviation safety is maintained.
- Compliance and Audits: MROs will need to comply with the new regulations and may be subject to audits by EASA to ensure adherence to Part-IS requirements.
- Training and Awareness: Personnel within MRO organizations must be trained and made aware of information security practices and protocols. This is crucial for maintaining a secure environment.

REGULATION (EU) 2023/203

Regulation (EU) 2023/203 lays down rules for the application of Regulation (EU) 2018/1139, focusing on the management of information security risks that could impact aviation safety. It introduces specific cybersecurity risk management measures that aviation entities must incorporate into their operations. These measures directly impact maintenance environments, aircraft systems, and IT/OT infrastructures, requiring organizations to adopt a systematic approach to cybersecurity compliance.

Regulation (EU) 2023/203 mandates several key requirements for aviation organizations and competent authorities to manage information security risks:

- Information Security Management Systems (ISMS): Organizations must establish and maintain ISMS that integrates cybersecurity into safety risk management frameworks.
- Implementation of structured cybersecurity risk assessment covering IT (Information Technology) and OT (Operational Technology) systems such as Aircraft Health Monitoring Systems (AHMS) and Maintenance, Repair, and Overhaul (MRO) software.
- Regular cybersecurity training and awareness programs tailored to aviation maintenance staff in compliance with Regulation (EU) 2023/203.
- Stricter requirements for cybersecurity risk management in aviation supply chains.
- Third-party vendors are required to adhere to strict cybersecurity standards (e.g., ISO 27001, NIST cybersecurity framework), as mandated by Regulation (EU) 2023/203.
- Aviation entities to implement structured incident response procedures and ensure timely reporting of cyber incidents.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

An Information Security Management System (ISMS) is a framework tool designed for organizations to enhance the security of their information, data, and systems. An ISMS includes various components, from the people in organization to technical security measures. For aviation MRO organizations, implementing an ISMS is crucial to protect against cyber threats and ensure compliance with regulations like EASA Part-IS.

The primary objective of this system is to limit the impact of security breaches and make sure the confidentiality, integrity, and availability of data by implementing risk management processes, security controls, and policies.

RISK IDENTIFICATION

This initial stage involves identifying the organization's critical assets, potential threats, and vulnerabilities. It includes understanding what data, systems, or other assets are crucial to the organization and what risks they face.

RISK ASSESSMENT

Once risks are identified, they need to be assessed to determine their potential impact and likelihood. This involves evaluating the severity of each risk and prioritizing them based on their potential to harm the organization. [**Figure 10-2**]

RISK MANAGEMENT STRATEGY

Once a risk has been assessed and analyzed, an organization will need to select treatment options:

- Remediation: Implementing a control that fully or nearly fully fixes the underlying risk.
  Example: You have identified a vulnerability on a server where critical assets are stored, and you apply a patch for that vulnerability.
- Mitigation: Lessening the likelihood and/or impact of the risk, but not fixing it entirely.

Figure 10-2. The stages of information security management.

Example: You have identified a vulnerability on a server where critical assets are stored, but instead of patching the vulnerability, you implement a firewall rule that only allows specific systems to communicate with the vulnerable service on the server.

- Transference: Transferring the risk to another entity so your organization can recover from incurred costs of the risk being realized.
  Example: You purchase insurance that will cover any losses that would be incurred if vulnerable systems are exploited. (Note: this should be used to supplement risk remediation and mitigation but not replace them altogether.)
- Risk acceptance: Not fixing the risk. This is appropriate in cases where the risk is clearly low and the time and effort it takes to fix the risk costs more than the costs that would be incurred if the risk were to be realized.
  Example: You have identified a vulnerability on a server but concluded that there is nothing sensitive on that server; it cannot be used as an entry point to access other critical assets, and a successful exploit of the vulnerability is very complex. As a result, you decide you do not need to spend time and resources to fix the vulnerability.
- Risk avoidance: Removing all exposure to an identified risk.
  Example: You have identified servers with operating systems (OS) that are about to reach end-of-life and will no longer receive security patches from the OS creator. These servers process and store both sensitive and non-sensitive data. To avoid the risk of sensitive data being compromised, you quickly migrate that sensitive data to newer, patchable servers. The servers continue to run and process non-sensitive data while a plan is developed to decommission them and migrate non-sensitive data to other servers.

This page was intentionally left blank.

Question 10-1
What is the greatest objective of aviation cybersecurity?

Question 10-2
While preparing to perform a task on an aircraft, you are handed an unknown ipad or laptop. What is your first concern?

Question 10-3
Name some ways in which an organization can help prevent cyber attacks.

Question 10-4
What is critical for an organization which has suffered a cyber attack?

Question 10-5
What is the basis of Regulation 2023/203?

Question 10-6
What are the three basic steps of a risk management strategy?

SUBMODULE 10 PRACTICE ANSWERS

Answer 10-1
To safeguard an aircraft's operation and navigation systems while in flight.

Answer 10-2
Has that device been affected by a cyber attack.

Answer 10-3
Isolate devices from other, regular software updates, Intrusion detection and prevention systems (IDPS), regular security audits, employee training.

Answer 10-4
That a previously defined response plan exists within the organization to contain the attack.

Answer 10-5
Regulation 2023/203 specifies EASA's cybersecurity requirements within aviation organizations.

Answer 10-6
- Identify the possible risks.
- Determine level of danger of each risk.
- Devise methods to prevent or reduce the risk.