

ISMS & Cyber 145 Workshop September 2026

- Practical Part-IS Implementation for Small_ & Medium Part-145s
- 7 Major ISMS-Cyber Exposures within an EASA Part 145 Organisation
- Potential Overreach by the CMM
- Considering Competency Assessments for Cybersecurity Staff and Best Practices to Upskill the Audit Staff who have no Cybersecurity Skills.
- Considering EASA Part 145 Minimum Training, Competence, and Awareness Requirements To be established for Maintenance Engineers, Certifying Staff, Quality, Safety, and Training Personnel.
- Considering ISMS Relationships within an EASA Part 145 Organisation - Safety vs. Security (SMS & ISMS Integration) & Security and Information Security interaction
- EASA Regulatory Oversight of EASA Part 145 ISMS & Cyber System
- How Can Cybersecurity be Integrated into an SMS System for a Country that has not yet Adopted Part IS?
- Human Failure the Major Source of Cyber Threat within an EASA Part 145 Organisation
- Information Security & Cyber Reporting Challenges within an EASA Part 145 Organisation
- Key Cybersecurity Challenges for EASA MRO Organisations
- Practical aspects of integrating Part-IS with SMS in a Part-145 organisation, with focus on understanding how information security events may affect aviation safety.
- Strategic Integration of Information Security Management Systems (ISMS) in EASA Part 145 Organisations

Practical Part-IS Implementation for Small_ & Medium Part-145s

What is the most practical approach for a small or medium-sized EASA Part-145 maintenance organisation to implement Part-IS requirements without establishing a separate dedicated cybersecurity department?

Practical Part-IS Implementation for Small/Medium Part-145s

A small or medium-sized Part-145 organization can achieve compliance without building a dedicated cybersecurity department by leveraging regulatory flexibility regarding proportionality, integration, and third-party support.

Key Implementation Strategies

SMS & Management System Integration (IS.I.OR.200)

- **Unified Risk Architecture:** Embed information security risk assessments directly into the existing Safety Management System (SMS) framework using bow-tie risk models.
 - Map cyber threat vectors, such as malware on portable maintenance tools or corrupted software load files, directly to traditional aircraft safety hazards.

- **Merged Occurrence Reporting:** Expand the Part-145 internal safety reporting scheme to collect information security events (e.g., unauthorized network connections, anomalous maintenance software behavior, lost smart tools, or phishing attempts) alongside standard safety occurrences under Regulation (EU) No 376/2014.
- **Integrated Documentation:** Incorporate Information Security Management Manual (ISMM) procedures directly into the existing Safety Management Manual (SMM) or Maintenance Organisation Exposition (MOE) to minimize administrative duplication.
 - Utilize existing SMS risk assessment structures (such as bow-tie models), occurrence reporting channels, and management review frameworks to incorporate information security risks that impact aviation safety.
- **Compliance Monitoring Safeguards:** To satisfy IS.I.OR.200(a)(12), the compliance monitoring (internal audit) function must remain strictly independent of operational ISMS management. If an operational manager oversees the ISMS, internal audits of the ISMS must be conducted by an independent peer, an internal auditor outside the ISMS chain, or a qualified third-party auditor.
- **Dual Roles:** Assign Part-IS roles and accountabilities to existing personnel (e.g., designating the Quality or Safety Manager to oversee ISMS implementation).
 - Part-IS permits assigning multiple administrative responsibilities to a single individual. A small or medium Part-145 can designate an existing key manager (such as the Quality Manager, Safety Manager, or IT Lead) to manage operational ISMS duties without hiring a dedicated Chief Information Security Officer (CISO).
- **Outsourcing Specialized Technical Tasks:** Contract specialized technical activities, such as continuous network monitoring, vulnerability scanning, security operations centre (SOC) functions, or technical risk assessments, to Managed Security Service Providers (MSSPs).
- **Supplier Prior Assessment:** Before contracting any ISMS activities, perform a documented evaluation of the supplier's technical competence, security credentials (e.g., ISO/IEC 27001 certifications), and operational stability.
- **Contractual Audit Rights & SLAs:** Include clear Service Level Agreements (SLAs), mandatory cyber-event reporting timelines, and explicit audit rights within service contracts so your organization can verify the supplier's performance.

Note - The Accountable Manager retains ultimate regulatory accountability and oversight of all contracted activities under IS.I.OR.235.

- The Part-145 Accountable Manager must formally endorse the Information Security Policy, ensure adequate resource allocation, and review ISMS performance during routine management reviews.

7 Major ISMS-Cyber Exposures within an EASA Part 145 Organisation

The transition toward highly digitized maintenance environments offers unprecedented efficiency for EASA Part 145 organizations, but it simultaneously introduces profound cyber-safety risks.

Addressing these major exposures, ranging from sophisticated ransomware and supply chain vulnerabilities to human factors and legacy equipment is essential.

By implementing a proactive, comprehensive Information Security Management System, MROs can ensure that their digital tools enhance, rather than compromise, the absolute safety of the flying public.

1. Escalating Cybersecurity Threats

- The aviation sector is facing a sharply rising tide of cyberattacks, with threat actors utilizing increasingly sophisticated methods.
- For an EASA Part 145 organization, the primary vectors include data breaches, targeted ransomware attacks, and denial-of-service disruptions.
- These threats extend far beyond mere IT inconveniences; they pose direct risks to the aircraft maintenance environment. If ransomware locks critical, electronic task cards, or parts inventory systems, the organization may be forced to halt operations.

2. Compromised Data Integrity and Availability

- Aviation safety relies fundamentally on the continuous, accurate, and reliable exchange of data between operators, MRO service providers, OEMs, and regulators. In a Part 145 context, data integrity is absolute: a technician must trust the electronic maintenance manuals, work orders, and digital sign-offs.
- If a cyber intrusion subtly alters maintenance history records, the resulting loss of data integrity could lead directly to catastrophic physical operational failures.
- Ensuring high availability of these systems is equally critical, as technicians cannot legally or safely release an aircraft to service without access to verified, uncorrupted maintenance data.

3. Cross-Domain Impact in a System-of-Systems

- Aviation operates as a massive "system-of-systems." An information security breach within one isolated domain, such as a third-party maintenance facility, can cascade unpredictably into other critical aviation systems.
- A compromised laptop used by a maintenance technician to download flight data or update aircraft software can potentially act as a bridge, transferring malware directly into the aircraft's avionics.
- Because of this interconnectedness, EASA regulations strongly emphasize the need for end-to-end risk management.
- Part 145 organizations cannot view their ISMS in a vacuum; they must account for how their digital footprint interfaces with the broader aviation ecosystem.

4. Human Performance and Operator Errors

- Despite advanced technological defenses, the human element remains one of the most significant vulnerabilities in any ISMS.
- Human factors contribute extensively to both the initiation of cybersecurity incidents and the failure to respond to them effectively.

- In a busy hangar, a technician might bypass security protocols to save time, use unauthorized USB drives to transfer data to aircraft systems, or fall victim to targeted phishing emails.
- Training and competence building are foundational elements of a functional ISMS. EASA Part 145 organizations must foster a culture where cyber hygiene is treated with the same rigor as physical tool control and foreign object debris (FOD) prevention.

5. Regulatory Complexity and Compliance Friction

- MROs face significant regulatory complexity. There is heavy overlap between aviation-specific ISMS regulations (like EASA Part-IS), broader cybersecurity directives (such as the NIS2 Directive in Europe), and data protection laws (like GDPR).
- Attempting to harmonize these various requirements with established international standards such as ISO 27001 and the NIST Cybersecurity Framework is a necessary but highly complex endeavor.
- For Part 145 organizations, mapping technical maintenance procedures to these abstract cybersecurity frameworks requires specialized expertise, often resulting in compliance fatigue and administrative overhead that can distract from core safety tasks.

6. Third-Party and Supply Chain Risk Management

- Part 145 organizations rarely operate independently; they rely on a vast network of subcontractors, parts suppliers, calibration labs, and IT service providers.
- This extensive outsourcing dramatically increases the organization's cyber attack surface.
- A breach at a smaller, less secure supplier can easily provide a backdoor into the primary MRO's network.
- Recognizing this vulnerability, EASA regulations explicitly require strict contractual obligations and continuous oversight of third-party providers.
- MROs must audit their suppliers' ISMS practices, ensuring that outsourced IT services and maintenance subcontractors adhere to the same stringent cybersecurity standards as the parent organization.

7. Legacy Maintenance Equipment and Tooling Vulnerabilities

- A unique exposure within Part 145 organizations involves the reliance on legacy diagnostic tools and ground support equipment.
- Many automated test equipment (ATE) stations, portable data loaders, and specialized diagnostic laptops run on outdated operating systems that are no longer supported or patched by the manufacturer.
- These legacy systems are frequently required to interface with older aircraft models but lack modern security controls. Integrating these highly vulnerable legacy tools into a modern ISMS requires creative risk mitigation strategies, such as air-gapping the equipment or using strict network segmentation, to ensure they do not become an easy entry point for malicious actors.

Potential Overreach by the CMM

Today's Story concerns over-reach by an EASA Compliant Monitoring Manager (CMM)

How detailed should MOE 3A be? I have a finding from our CMM that my Chapter 3A and attached procedures are very complicated, and now I am reducing the text to make it simpler by removing details, additional procedures and registers forms.

Sofema Aviation Opinion

Raising a formal audit finding simply because MOE Chapter 3A is "too complicated" represents a clear overreach of the Compliance Monitoring Manager's (CMM) regulatory role.

Moreover stripping out required procedures, registers, and forms to resolve findings related to opinion (subjective—not prescriptive) it creates severe compliance exposure under EASA rules.

CMM Role Overreach vs. Regulatory Responsibilities

Misapplication of Audit Findings: Under EASA Part-145 and Part-IS oversight rules (IS.I.OR.200(a)(12)), the CMM's mandate is to monitor compliance against legal requirements and approved exposition procedures, evaluating whether processes are effective and compliant.

A formal non-compliance finding must cite a specific breach of a regulation or approved MOE standard, not a subjective opinion on procedural writing style or complexity.

- **Confusing Quality Control with Audit Oversight:** The CMM is responsible for independent compliance monitoring. Dictating procedural design or demanding the removal of operational details blurs the line between independent auditing and operational management, undermining the CMM's objectivity.

Required Level of Detail for MOE Chapter 3A

- **Mandatory Process Documentation:** Part-IS (IS.I.OR.200(c) and IS.I.OR.250) mandates that an organization document all key processes, procedures, roles, and responsibilities required to manage safety-impacting information security risks. MOE Chapter 3A must be detailed enough to ensure processes are repeatable, reproducible, and verifiable during an EASA audit.
- **Essential Documentation Artifacts:** AMC1 IS.I.OR.200(c) and IS.I.OR.245 require specific documented information, including risk registers (ledgers), interface management procedures, internal/external incident reporting schemes, and record-keeping forms.

The Risks of Over-Simplification

- **Creating Regulatory Non-Compliance:** Removing sub-procedures, forms, and risk registers to make the text "simpler" removes the objective evidence EASA inspectors look for to confirm an active Information Security Management System (ISMS). High-level text without granular procedures leaves front-line staff without clear operational guidance.
- **Loss of Auditability:** Standardized forms and registers (such as threat scenario tracking or risk treatment plans) are necessary to prove that risk assessments and corrective actions are being systematically executed.

Mitigation - Consideration for a Possible Path Forward

- **Reclassify the Finding:** Request that the CMM reclassify the finding from a non-compliance finding to an internal Opportunity for Improvement (OFI) focused on document readability rather than regulatory breach.

- **Streamline Without Deleting:** Improve clarity by using visual flowcharts, process maps, or modular appendices for detailed sub-procedures, forms, and registers—ensuring full procedural details remain intact and referenced in MOE 3A without stripping mandatory Part-IS compliance controls.

Considering Competency Assessments for Cybersecurity Staff and Best Practices to Upskill the Audit Staff who have no Cybersecurity Skills.

Sofema Aviation considers key challenges to be addressed during the implementation of ISMS & Cyber Security within an EASA Part 145

Introduction

Implementing Part-IS within an EASA Part-145 maintenance organisation requires integrating cybersecurity governance directly into airworthiness safety management.

Evaluating cybersecurity personnel and upskilling traditional quality auditors demands a structured competency framework tailored to maintenance environments.

Cybersecurity Staff Competency Assessment & Development

- Customizing framework alignment and role mapping under EASA Part-IS requires blending standard Information Technology / Operational Technology IT/OT cybersecurity competencies with domain-specific Part-145 maintenance airworthiness responsibilities. To execute this effectively within a maintenance organisation, apply the following operational guidance:

Leverage Part-IS Appendix II Mappings

- Use Appendix II of Part-IS (Part-IS.I.OR) as your starting baseline, as EASA has directly mapped core Part-IS tasks—such as risk assessment, incident response, and vendor oversight—to NIST CSF function categories and ISO/IEC 27001 controls. (see Sofema Library for Appendix II) (*Aviation Information Security and Cyber Security*)
- Translate these high-level regulatory tasks into clear operational job duties before referencing external frameworks.

Adapt Generic Frameworks to Maintenance Assets

- Recognize that standard frameworks like NIST NICE or ENISA's European Cybersecurity Skills Framework (ECSF) focus primarily on standard IT environments and lack an integrated aviation safety context.
- Tailor mapped Knowledge, Skills, and Abilities (KSAs) to include specialized maintenance assets, such as Electronic Flight Bag (EFB) load software tools, automated test equipment, ground support systems, and MRO software platforms.

Define Discrete Maintenance-Cyber Roles

Information Security Lead / CISO: Map against ECSF management profiles (e.g., Information Security Manager), but mandate additional knowledge of EASA safety risk management and bow-tie risk methodologies.

Cyber Operations & Systems Administrators: Map to NICE Technical Support and Security Provision roles, focusing specifically on access controls, network segmentation, patch management, and software integrity for MRO systems.

Maintenance Technicians & Certifying Staff: Define frontline operational roles requiring KSAs around secure data transfer, media hygiene (USB/portable tools), and internal reporting of suspicious electronic interactions.

Quality Compliance Auditors: Map to oversight functions, focusing on verifying ISMS compliance and process adherence rather than performing technical engineering testing.

Execute Role-Based Knowledge, Skills, and Abilities KSA Gap Assessments

- Assess each staff member's verified qualifications, past experience, and formal training against the customized role profile to isolate specific competency deficits.
- Differentiate between gaps in technical cyber skills and gaps in aviation safety awareness to ensure targeted training or recruitment.

Competency Gap Analysis: Conduct initial evaluations of personnel qualifications, formal certifications (e.g., CISSP, CISM, ISO 27001), and practical experience to identify specific knowledge gaps relative to assigned duties.

Aviation Safety Integration: Evaluate staff on their ability to link cyber threats to physical aircraft safety outcomes using Bow-Tie risk modeling, ensuring they understand how compromised maintenance data or software loading impacts airworthiness.

Identity & Trustworthiness Verification: Confirm identity through documentary evidence and verify trustworthiness via formal background checks, education verification, and criminal record reviews prior to granting access to critical systems. Staff must formally acknowledge their assigned responsibilities in a traceable manner.

Targeted Qualification Pathways: Bridge identified competency gaps through structured learning programs, combining formal technical training, professional certification recognition, and on-the-job maintenance domain exposure.

Continuous Assessment & Re-evaluation: Periodically review staff competencies and training programs to account for evolving cyber threats, emerging maintenance technologies, and system architecture changes.

Upskilling Non-Technical Audit Staff

Part-145 quality auditors maintain compliance monitoring oversight under IS.I.OR.200(a)(12). Performing a regulatory compliance audit does not require the auditor to be a technical cybersecurity

Subject Matter Expert (SME). Instead, the auditor must be competent in audit methodology and capable of interpreting regulatory obligations to verify that processes and evidence conform to EASA requirements.

- **Phase 1: Regulatory Interpretation & Literacy:** Deliver structured training on Part-IS regulatory obligations, demystifying technical jargon and establishing core ISMS concepts (ISO/IEC 27001/27002) so auditors can interpret compliance criteria without requiring technical execution skills.
- **Phase 2: Safety & Operational Context:** Educate auditors on where regulatory requirements apply within routine Part-145 operations, such as ground support equipment, software supply chains, calibration tool integrity, and vendor access management.
- **Phase 3: Objective Audit Toolkits:** Provide auditors with standardized checklists, sampling templates, and non-technical evidence criteria (e.g., verifying access control lists, background check documentation, supplier contract clauses, and incident drill logs).
- **Phase 4: Guided Co-Auditing & Mentorship:** Pair quality auditors with cybersecurity SMEs during initial implementation cycles. This provides hands-on experience in evaluating technical evidence against regulatory obligations without placing the burden of SME-level analysis on the auditor.
- **Phase 5: Continuous Capability Building:** Conduct periodic refresher sessions, scenario walkthroughs, and practical workshops to ensure auditors maintain strong regulatory evaluation capabilities as Part-IS processes mature.

Considering EASA Part 145 Minimum Training, Competence, and Awareness Requirements To be established for Maintenance Engineers, Certifying Staff, Quality, Safety, and Training Personnel.

Sofema Aviation (SA) Considers how to demonstrate Part-IS compliance during an EASA audit, a Part-145 maintenance organization must establish role-based competence criteria, conduct targeted initial and recurrent training, and maintain traceable personnel records.

Role-Specific Competence & Training Baselines

Maintenance Engineers & Certifying Staff

- **Security Awareness & Threat Recognition:** Personnel must complete regular awareness sessions covering basic cyber hygiene, social engineering, phishing, and recognizing unauthorized electronic interactions.
 - They must be trained to detect physical or digital tampering on maintenance systems, ground support equipment, and aircraft interfaces.

- **Operational & Technical Controls:** Staff must demonstrate competence in the secure handling of portable maintenance devices, electronic tech logs, software loading media, and ground support software.
 - Training must emphasize adherence to safe software distribution processes and manufacturer instructions to maintain system integrity during updates.
- **Internal Event Reporting:** Engineers and certifying staff must understand the internal reporting scheme established under point IS.I.OR.215.
 - They must be capable of immediately reporting software anomalies, compromised maintenance tools, data corruption, or suspected cybersecurity events without fear of punitive action under Just Culture principles.

Quality & Safety Personnel

- **Auditing & Compliance Monitoring:** Quality auditors must possess specific competence to evaluate Information Security Management System (ISMS) processes, audit technical information security controls, and verify compliance with Part-IS requirements.
 - They must also be qualified to audit contracted activities, evaluating the technical competence, security posture, and performance of Managed Security Service Providers (MSSPs) and third-party software vendors.
- **Safety Risk Assessment Integration:** Safety personnel must understand how to combine information security risk assessments with traditional Safety Management System (SMS) processes using interlinked bow-tie risk models.
 - They require competence to identify cyber-threat vectors, perform root-cause analyses on information security incidents, and evaluate risk treatment measures that impact aircraft structural or system integrity.
- **Vulnerability & Incident Management:** Quality and safety teams must be trained to assess the exploitability of reported vulnerabilities, monitor supplier risk notifications, and coordinate corrective actions for identified deficiencies.

Training Personnel

- **Program Development & Competence Mapping:** Training managers and instructors must be capable of identifying organizational competence gaps by evaluating work roles against required knowledge, skills, and abilities. They must be trained to utilize recognized cybersecurity frameworks—such as the NIST Cybersecurity Framework (NIST CSF), National Initiative for Cybersecurity Education (NICE), or ENISA European Cybersecurity Skills Framework (ECSF), to establish baseline competencies mapped to Part-IS main tasks listed in Appendix II.
- **Curriculum Maintenance & Review:** Training staff must periodically review and update training delivery methods (e.g., classroom, e-learning, on-the-job training) and course content to reflect

evolving cyber threat landscapes, technological changes, and lessons learned from internal security occurrences.

Key Audit Evidence Required by EASA

To verify compliance during oversight audits, EASA auditors will inspect specific documented artifacts to confirm that personnel requirements under point IS.I.OR.240 and record-keeping mandates under point IS.I.OR.245 are fully satisfied.

- **Competence Gap Analysis:** Documented evidence demonstrating that the organization has mapped assigned work roles to required knowledge, skills, and abilities, identified existing qualification gaps, and implemented targeted learning plans to bridge those gaps.
- **Traceable Acknowledgments:** Verifiable records, such as wet signatures, digital signatures, or system-logged email confirmations, proving that every employee has formally acknowledged receipt, understanding, and acceptance of their assigned information security roles and responsibilities.
- **Trustworthiness & Identity Verification:** Documented procedures and criteria used to verify employee identity through documentary evidence and establish trustworthiness prior to granting access to critical aviation systems or data.
 - This includes background checks, verification of employment history, absence of criminal records (or equivalent certificates of good conduct), and ongoing monitoring of conduct.
- **Qualification & Training Records:** Comprehensive individual training records containing certificates, qualifications, and evidence of experience.
 - These records must be retained for the entire duration of the individual's employment and for at least 3 years after the person leaves the organization.

Summary Breakdown of Personnel Requirements

- **Maintenance & Certifying Staff Baseline:** Focused on cyber hygiene, software loading security, tool tampering detection, and internal event reporting.
 - Primary audit evidence includes training completion logs, signed responsibility acknowledgments, and event reporting records.
- **Quality & Safety Personnel Baseline:** Focused on ISMS internal auditing, MSSP vendor oversight, bow-tie risk integration, and root-cause investigation.
 - Primary audit evidence includes internal ISMS audit reports, supplier assessment logs, and bow-tie risk assessment registers.
- **Training Personnel Baseline:** Focused on competence gap mapping (NIST/ENISA frameworks), curriculum design, and periodic training review.

- Primary audit evidence includes documented gap analyses, training program review records, and framework mapping matrices.
- **All Personnel with System Access Baseline**: Focused on identity verification, adherence to need-to-know access controls, and Just Culture reporting.
 - Primary audit evidence includes identity documentation, background check files, and initial/recurrent awareness sign-off sheets.

Considering ISMS Relationships within an EASA Part 145 Organisation - Safety vs. Security (SMS & ISMS Integration) & Security and Information Security interaction

Sofema Aviation (SA) Takes a deep dive into ISMS organisational relationships

Introduction

Commission Implementing Regulation (EU) 2023/203 establishes a comprehensive European regulatory framework for managing information security risks with a potential impact on aviation safety.

- For an EASA Part-145 maintenance organisation, excluding those exclusively maintaining light aircraft under Part-ML, compliance with Annex II (Part-IS.I.OR) requires setting up, implementing, and maintaining an Information Security Management System (ISMS).
- Modern maintenance operations rely heavily on interconnected digital technologies, including computerized maintenance management systems (CMMS), electronic flight bags (EFBs), automated ground support equipment (GSE), diagnostic tooling, and software loading devices. Flaws in network and information systems can directly affect aircraft airworthiness and civil aviation safety.

Safety vs. Security: SMS & ISMS Integration

- **Conceptual Relationship & Dual Bow-Tie Dynamics** An EASA Part-145 organisation maintains a Safety Management System (SMS) in accordance with Regulation (EU) No 1321/2014 and Regulation (EU) 2018/1139 to manage safety risks arising primarily from random hardware failures, human error, or environmental factors.
- In contrast, an ISMS under Part-IS addresses information security threats where existing vulnerabilities in information assets could be exploited by actors with malicious intent or triggered by unauthorized electronic interactions.
- The operational interaction between SMS and ISMS is framed through interacting risk assessments including "bow-tie" (recommended). An information security threat scenario (e.g., malware injection into a maintenance laptop or software supply chain compromise) acts upon an information security hazard to create an information security top event (e.g., corrupted aircraft software binary or compromised maintenance data).
- This information security consequence directly feeds into the safety bow-tie as a safety threat, leading to a safety hazard (e.g., unpredictable flight control behavior or engine control disruption) and potential safety consequences such as aircraft accidents or incidents.

Key Challenges in SMS & ISMS Integration

- **Cultural Friction (Just Culture vs. Confidentiality):** SMS relies fundamentally on an open "Just Culture" where personnel are encouraged to report errors without fear of punishment.
 - Conversely, Part-IS mandates strict confidentiality and need-to-know controls to protect sensitive system vulnerabilities and threat intelligence from unauthorized disclosure. Reconciling an open reporting ethos with strict security confidentiality creates organizational friction.
- **Divergent Risk Assessment Methodologies:** Safety risk management historically assesses likelihood and severity using statistical probability derived from historical operating data.
 - Information security risk assessment relies on evaluating threat actor capabilities, exploitability, and dynamic attack vectors where traditional statistical probability models are inadequate.
- **Skill Set & Departmental Silos:** Safety managers and maintenance engineers typically lack deep cybersecurity expertise, whereas IT security staff often lack operational knowledge of airworthiness rules, aircraft functional chains, and maintenance procedures.
- **ISMS Scope Delineation:** A significant challenge for Part-145 organisations is defining the precise boundaries of the ISMS.
 - Over-extending the scope to cover general corporate IT creates excessive regulatory burden, while under-extending it leaves critical ground infrastructure, software loading tools, and component test benches exposed.

Best Practices for SMS & ISMS Integration

- **Unified Governance under Accountable Manager Oversight:** Part-IS requires the Information Security Policy to be endorsed by the Accountable Manager.
 - Part-145 organisations should integrate ISMS governance into existing executive safety review boards, establishing top-level accountability while ensuring safety and security objectives align with overall business operations.
- **Joint Risk Assessment - Bow-Tie Modeling & Shared Risk Registers:** Establishing multidisciplinary risk assessment teams, combining safety specialists, avionics engineers, and cybersecurity experts, enables the organisation to trace attack paths from digital entry points to safety impact.
 - Utilizing standardized risk acceptance matrices that map threat occurrence against ICAO safety severity categories ensures mutual comparability across departments.
- **Harmonized Internal Event Reporting:** Part-145 organisations should adapt their existing internal safety reporting schemes to capture information security events, anomalies, and software glitches.

- By anonymizing sensitive vulnerability details prior to broad internal dissemination, organisations uphold Just Culture principles while protecting critical security data.
- **Functional Chain Risk Information Sharing:** Maintenance organisations form a critical link in the aviation functional chain between suppliers/OEMs upstream and CAMOs/Air Operators downstream.
 - Part-145 entities may establish risk-sharing mechanisms to communicate residual information security risks to downstream operators, allowing them to evaluate the final impact on flight safety.

Security and Information Security Interactions

Interplay between Physical, Aviation, and Information Security Information security under Part-IS intersects directly with physical and civil aviation security frameworks governed by Regulation (EC) No 300/2008 and Regulation (EU) 2015/1998. In a maintenance environment, physical security controls (e.g., hangar access control, badging, physically secure server rooms) form the first line of defense for digital assets, including maintenance terminals, portable data loaders, and aircraft network access points.

Key Challenges in Security Interactions

- **Physical Access to Maintenance Attack Vectors:** Maintenance activities naturally require physical access to aircraft data buses, avionics bays, and ground support equipment. An unauthorized individual gaining physical access to an unattended maintenance laptop or USB loading device inside a hangar can bypass remote perimeter network defenses.
- **Supply Chain & Subcontractor Exposure:** Part-145 organisations depend on complex supply chains for software updates, calibrated tooling, component overhaul, and outsourced IT services.
 - A compromise in a vendor's software repository or managed service provider (MSP) infrastructure can introduce corrupted binaries or malware directly into aircraft systems during routine maintenance.
- **Personnel Trustworthiness & Insider Threats:** Part-IS requires verifying the identity and trustworthiness of personnel accessing safety-impacting systems.
 - Reconciling standard aviation security background checks under Regulation (EU) 2015/1998 with Part-IS requirements for personnel with administrative or unsupervised access to maintenance IT assets introduces legal and administrative complexities.

Best Practices for Security & Information Security Synergy

- **Hardening Digital & Physical Maintenance Interfaces:** Part-145 organisations must enforce multi-factor authentication, role-based access control (RBAC), and encryption across all portable maintenance devices and software loaders.

- Dedicated, air-gapped staging terminals should be established to verify the digital signatures and integrity of OEM software updates before installation on aircraft avionics.
- **Robust Supply Chain Governance & Contractual Oversight:** Pursuant to point IS.I.OR.235, organisations must conduct formal prior risk assessments of external suppliers, MSPs, and contracted entities.
 - Contracts must mandate adherence to information security standards, right-to-audit privileges, and strict timelines for reporting security incidents.
- **Integrated Vetting & Security Awareness Programs:** Organisations should leverage existing aviation security background checks while applying enhanced screening for personnel holding high-level IT administrative rights or managing critical maintenance databases.
 - Continuous security awareness training should be embedded into standard human factors programs to train maintenance technicians to recognize social engineering, unauthorized hardware tampering, and suspicious system behaviors.
- **Centralized Event Monitoring & SOC Capabilities:** Implementing Security Information and Event Management (SIEM) solutions within a Security Operations Centre (SOC) enables the correlation of physical access logs with system network activity. Automated alert mechanisms allow rapid containment of anomalies, such as off-hours software uploads or unauthorized USB insertions, before operational safety is compromised.

Integrating SMS and ISMS through unified risk management, alongside aligning physical aviation security controls with digital defense mechanisms, allows an EASA Part-145 organisation to maintain high airworthiness standards while establishing full regulatory compliance under Part-IS.

EASA Regulatory Oversight of EASA Part 145 ISMS & Cyber System

Sofema Aviation Examines the 7 Key Inspection Areas & Expected Outcomes & checkpoints which are typically assessed during a regulatory oversight audit.

- The inspector applies MSAT criteria to score each area across four maturity tiers:
 - *Present* (policy exists),
 - *Suitable* (suited to AMO size/complexity),
 - *Operating* (actively practiced), and
 - *Effective* (delivering measurable risk reduction).

The expected outcome is a verified level of *Effective*, demonstrating that human-centric vulnerabilities are systematically controlled and digital vigilance matches operational speed.

Introduction

An EASA inspector evaluating a Part 145 Approved Maintenance Organization (AMO) under Regulation (EU) 2023/203 (Part-IS) May use the Management System Assessment Tool (MSAT) to measure whether security controls are not just documented, but actively effective in mitigating operational threats, particularly the 80% of cyber breaches driven by human failure.

1. Governance & SMS-ISMS Integration

- *Focus:* Alignment between the Safety Management System (SMS) and the Information Security Management System (ISMS), accountability of the Accountable Manager, and integration of digital risk into overall airworthiness risk.
- *Outcome:* Security decisions are backed by executive leadership, and cyber threats are systematically evaluated for their direct impact on aircraft safety.

2. Cyber "Just Culture" & Reporting

- *Focus:* Psychological safety regarding digital mistakes, ensuring technicians report accidental link clicks, lost credentials, or suspicious system behavior without fear of reprisal.
- *Outcome:* Elimination of the cyber reporting gap, enabling rapid internal containment of human error before escalation.

3. Role-Tailored Competence & Awareness

- *Focus:* Moving beyond generic compliance quizzes to role-specific training, phishing simulations, and social engineering defenses targeting maintenance planners, procurement, and line technicians.
- *Outcome:* Staff actively recognize Business Email Compromise (BEC), spoofed supplier communications, and phone-based pretexting targeting MRO platforms (e.g., AMOS, Maintenix).

4. Information Security Risk Assessment & Asset Mapping

- *Focus:* Identification of critical digital assets, legacy Operational Technology (OT), avionics test benches, and Ground Support Equipment (GSE).
- *Outcome:* Comprehensive risk registers that map physical airworthiness threats directly to digital vectors, aligned with ENISA threat intelligence.

5. Technical Mitigations & Access Control

- *Focus:* Implementation of hardware USB sanitization kiosks, Endpoint Detection and Response (EDR) on line laptops, and strict credential management.
- *Outcome:* Mitigation of unsanitized removable media risks on flight hardware/GSE and enforcement of mandatory Multi-Factor Authentication (MFA) across all organizational portals.

6. Supply Chain & Interconnectedness Management

- *Focus:* Oversight of component repair stations, OEMs, third-party software vendors, and remote access backdoors.
- *Outcome:* Zero-Trust access controls, strict third-party data boundaries, and continuous verification of vendor security posture.

7. Incident Response, Continuous Improvement & Auditing

- *Focus:* Detection capability, root-cause analysis of cyber events, and periodic internal audits using MSAT indicators.
- *Outcome:* Proven capability to contain breaches, feed lessons learned back into training, and continuously refine Part-IS processes.

Summary

Achieving a successful EASA Part-IS audit under Regulation (EU) 2023/203 requires Approved Maintenance Organizations to shift from static, paper-based compliance to active, measurable operational resilience.

By evaluating the seven key inspection areas through the Management System Assessment Tool (MSAT), regulators look past basic policy existence to verify that cyber safeguards are operating effectively to protect aircraft safety.

To secure an Effective rating across all MSAT maturity tiers, Part 145 organizations must focus on three strategic pillars:

- **Unified Governance & Just Culture:** Integrating ISMS into the existing Safety Management System (SMS) embeds digital risk directly into overall airworthiness oversight. Extending psychological safety into the cyber domain closes the reporting gap, encouraging technicians to report digital errors without fear and directly addressing the human factor driving 80% of cyber breaches.
- **Targeted Competence & Asset Visibility:** Broad, generic awareness is replaced by role-tailored defenses for planners, procurement, and technicians. Grounding this training in comprehensive asset mapping—from avionics test benches to MRO platforms—ensures staff can actively identify and intercept specialized threats like Business Email Compromise and software supply chain exploits.
- **Proactive Technical Safeguards:** Implementing strict zero-trust parameters, mandatory MFA, USB sanitization kiosks, and continuous vendor oversight closes external entry points before legacy equipment or third-party interconnections can compromise flight hardware.

Part-IS compliance using the MSAT framework is not a static checkbox exercise, it is a continuous operational standard. By embedding cyber vigilance into daily maintenance routines, AMOs ensure that digital risk management moves at the same speed as maintenance operations, safeguarding aircraft integrity in an increasingly interconnected world.

How Can Cybersecurity be Integrated into an SMS System for a Country that has not yet Adopted Part IS?

Sofema Aviation Considers a number of challenges related to the implementation of a ISMS & Cyber Management System,

Third-country organizations holding EASA approvals must comply directly with EASA Part-IS requirements (Part-IS.I.OR) overseen by EASA as their competent authority, regardless of whether their local National Aviation Authority has adopted Part-IS rules.

Organizations can satisfy these requirements by extending their existing ICAO - or EASA-compliant Safety Management System (SMS) to manage information security risks that pose a potential impact on aviation safety.

Governance & Organizational Structure

- **Unified Leadership:** Leverage the existing SMS Accountable Manager and governance structures to oversee information security policies, ensuring clear executive accountability without creating a duplicate management system.
- **Policy Expansion:** Adapt the overarching safety policy to include explicit commitments to identifying, managing, and mitigating cybersecurity threats across operational and maintenance technology.

Integrated Safety Risk Management

- **Bow-Tie Methodology:** Interlink information security risk assessments with safety risk assessments using bow-tie models. Information security threats (e.g., malware, unauthorized electronic interaction, data corruption) act as threat vectors that can breach preventive barriers and lead to traditional safety top events.
- **Combined Risk Classification:** Align information security risk matrices with existing SMS safety criteria, evaluating threat likelihood against the severity of potential safety consequences (negligible, incident, or accident) to determine acceptable versus unacceptable risks.

Reporting Schemes & Incident Response

- **Integrated Occurrence Reporting:** Extend the organization's SMS internal reporting scheme to enable staff to report cyber events, system anomalies, and software vulnerabilities alongside traditional safety hazards.
- **Synchronized Emergency Plans:** Merge cybersecurity incident response procedures into the existing SMS Emergency Response Plan (ERP), establishing pre-defined containment, recovery time objectives, and operational fallback modes.

Supply Chain & Interface Management

- **Functional Chain Mapping:** Identify physical and logical interfaces with external entities (e.g., software providers, maintenance vendors, data services) to evaluate mutual risk exposure.

- **Contractual Mandates:** Enforce mandatory cybersecurity event reporting and audit rights in third-party contracts to ensure sub-contractors do not introduce unmanaged safety risks.

Compliance Monitoring & Continuous Improvement

- **Combined Auditing:** Expand the SMS compliance monitoring function to perform routine internal audits of information security controls and system configurations.
- **Maturity & Feedback:** Utilize findings from cyber audits, vulnerability evaluations, and incident investigations to drive continuous improvement within both the SMS and ISMS frameworks.

Human Failure the Major Source of Cyber Threat within an EASA Part 145 Organisation

Sofema Aviation (SA) Considers the exposure caused by Human Failure together with appropriate mitigations

Introduction

Empiric evidence indicates that 80% of cybersecurity breaches stem from human failure aligns directly with threat intelligence data where social engineering, credential theft, and human error represent the primary attack surface.

See the Following - (<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>)

Within an EASA Part 145 Approved Maintenance Organization (AMO), where culture and engineering training naturally focus on physical airworthiness, digital vigilance can easily lag behind operational speed.

Validating the Human Factor with Real-World Vectors

- **Phishing & Business Email Compromise:** Threat actors routinely target maintenance planners and procurement teams with spoofed emails posing as parts suppliers (OEMs) or regulatory authorities.
 - The goal is usually stealing login credentials for MRO software (e.g., AMOS, Maintenix) or intercepting wire transfers for high-value components.
- **Unsanitized Removable Media:** Maintenance engineers using USB drives or portable laptops to transfer avionics logs, engine diagnostic software, and digital Aircraft Maintenance Manual (AMM) updates.
 - Plugging an infected drive into Ground Support Equipment (GSE) or aircraft-connected laptops creates a direct pathway for malware or ransomware.
- **Credential Reuse & Pretexting:** Shift rotations, shared workstations, and urgent turnaround times increase the likelihood of weak passwords or personnel succumbing to phone-based social engineering (pretexting) impersonating IT helpdesks.

Typical Exposures in EASA Part 145

- **Legacy Operational Technology (OT):** Avionics test benches and workshop machinery often run legacy, unpatched operating systems that sit on the boundary of modern IT networks.
- **Supply Chain Interconnectedness:** Subcontractors, component repair stations, and third-party software vendors often have elevated remote access to inventory and maintenance records, making them a backdoor entry point.
- **SMS vs. ISMS Friction:** Safety Management Systems (SMS) historically treat error as a learning tool, but staff often fail to report a cyber mistake (like clicking a malicious link) creating a dangerous reporting gap.

Mitigations and EASA Part-IS Alignment Under EASA Regulation (EU) 2023/203 (Part-IS), AMOs must integrate an Information Security Management System (ISMS) into their existing SMS framework. Effective mitigations include:

- **Cyber "Just Culture":** Extending physical SMS reporting principles so technicians feel safe immediately self-reporting clicked links, lost devices, or strange system behavior.
- **Role-Tailored Training:** Moving past generic compliance quizzes to run realistic, role-based phishing simulations and media-handling drills for line staff.
- **Technical Controls:** Implementing hardware USB-scanning kiosks (media sanitization), Multi-Factor Authentication (MFA) across all MRO portals, and Endpoint Detection and Response (EDR) on line-maintenance laptops.
- **Zero-Trust Vendor Management:** Enforcing strict access controls and regular security assessments for third-party suppliers connected to internal systems.

Information Security & Cyber Reporting Challenges within an EASA Part 145 Organisation

Sofema Aviation (SA) looks at the reporting challenges faced by the EASA Part 145 workforce and how to mitigate.

Introduction

Navigating information security reporting in an EASA Part 145 organization requires bridging traditional aviation safety management systems (SMS) with Information Security Management System (ISMS) protocols under Commission Implementing Regulation (EU) 2023/203 (Part-IS) and Regulation (EU) No 376/2014.

Key Challenges in Part 145 Cyber Reporting

- **Cultural and Skill Gaps:** Maintenance engineers are trained in physical airworthiness and human factors, making digital threat detection, less intuitive than physical component checks.

- **Alert Noise vs. Safety Signal:** Distinguishing thousands of daily automated network probes from targeted attacks aimed at critical maintenance software (e.g., AMOS, TRAX, or tooling calibration databases).
- **Cross-Domain Alignment:** Merging ISMS incident response timelines with SMS Just Culture principles without creating redundant reporting channels or discouraging staff from reporting human cyber errors.

Tiered Reporting Thresholds

- **No Need to Report:** Automated network noise blocked by perimeter controls with zero impact on operations, systems, or data.
 - Examples include generic phishing emails caught by spam filters, routine port scans, or malware blocked at the firewall. (These are logged automatically by security tools without manual intervention.)
- **Internal Reporting Only:** Suspicious events, employee slip-ups, or security incidents that do not directly threaten aircraft airworthiness or maintenance data integrity.
 - Examples include targeted spear-phishing attempts, lost encrypted laptops, unauthorized USB usage, or non-critical IT network disruptions. (Report these internally to the Information Security Officer (ISO) or ISMS team per internal SLA timelines.)
- **Competent Authority Reporting (376/2014 & Part-IS):** Confirmed cyber incidents that compromise or endanger aviation safety, airworthiness data, or critical maintenance equipment.
 - Examples include ransomware on maintenance databases, unauthorized modification of digital sign-offs, or compromised ground software loading systems. Submit a mandatory occurrence report to the National Competent Authority (NCA) or EASA within 72 hours.

Determining and Identifying the Need to Report

- **Anomaly & Event Detection:** Monitor networks and train maintenance personnel to flag unexpected system behaviors, unauthorized configuration changes, or suspicious data requests.
- **Triage & Impact Assessment:** Evaluate the event against two main metrics:
 - System Criticality (is the system used in maintenance planning, aircraft data loading, or airworthiness releases?) and
 - Data Integrity/Availability (has airworthiness data been modified or rendered inaccessible?).
- **Safety Threshold Check:** Determine if the incident affects, or could reasonably be expected to affect, the safety of flight operations or aircraft structural/systems integrity.

- **Regulatory Execution:** If the safety threshold is met, activate the combined ISMS/SMS notification channel to dispatch the initial 72-hour notification to the Competent Authority under Part-IS.I.OR.230 and Regulation (EU) No 376/2014.

Key Cybersecurity Challenges for EASA MRO Organisations

Under EASA Regulation (EU) 2023/203 (Part-IS), Part 145 Maintenance, Repair, and Overhaul (MRO) organisations are required to integrate an Information Security Management System (ISMS) alongside their Safety Management System (SMS), linking cybersecurity directly to airworthiness.

Sofema Aviation (SA) considers key exposures within the Information Security and cyber ECO System. Risk severity must ultimately be mapped directly into the organization's existing SMS safety matrix, treating any cyber threat that could compromise maintenance data accuracy, tools, or aircraft configuration as a potential direct hazard to flight safety.

Key Cybersecurity Challenges for MRO Organisations

- **Operational Technology (OT) & GSE Vulnerabilities:** Maintenance diagnostic tools, avionics data loading equipment, and automated Ground Support Equipment (GSE) frequently run on legacy software or unpatched operating systems, leaving them vulnerable to malware.
- **Complex Supply Chain Interfaces:** MROs continuously exchange maintenance data, Airworthiness Directives (ADs), and digital certifications with OEMs, CAMOs, and parts suppliers, exposing networks to supply chain breaches.
- **Competency & Culture Gaps:** Aircraft maintenance technicians are trained primarily for physical airworthiness rather than cyber hygiene, making shop-floor environments vulnerable to compromised USB drives, weak access controls, or social engineering.
- **SMS and ISMS Integration:** Harmonizing information security risk registers with existing SMS hazard logs creates organizational friction regarding accountability between Compliance, Safety, and IT departments.
- **Data Integrity of Maintenance Records:** Ensuring digital task cards, electronic signatures, and modification logs remain unalterable and audit-ready without disrupting fast-paced maintenance turnarounds.

Measuring Cybersecurity Risk in Part 145 Operations

Measuring cybersecurity risk in an MRO requires evaluating digital threats through an airworthiness lens using a safety-weighted risk formula:

$$\text{Information Risk} = \text{Threat Likelihood} \times \text{Vulnerability Severity} \times \text{Safety \& Operational Impact}$$

To effectively track and quantify this risk without complex matrices, MROs utilize Key Risk Indicators (KRIs) categorized across core operational areas:

- **Asset Vulnerability:** Track the percentage of unpatched GSE, diagnostic tools, and MRO software to measure physical-to-digital attack exposure on the hangar floor.

- **Supply Chain Security:** Measure the percentage of digital interface suppliers compliant with EASA Part-IS to quantify data contamination risk from third-party vendor networks.
- **Response Resilience:** Monitor Mean Time to Detect (MTTD) and Contain (MTTR) cyber incidents to evaluate containment speed before compromised data affects airworthiness releases.
- **Data Integrity:** Audit failure rates on electronic signatures and task card logs to ensure maintenance records remain tamper-proof and fully traceable.
- **Human Element:** Evaluate staff phishing simulation failure rates and Part-IS training completion to track workforce readiness against social engineering threats.

Practical aspects of integrating Part-IS with SMS in a Part-145 organisation, with focus on understanding how information security events may affect aviation safety.

Sofema Aviation considers key aspects related to the potential impact on Aviation Safety

Integrating EASA Part-IS into a Part-145 Safety Management System (SMS) bridges the gap between Information Technology & Operational Technology (IT/OT) security and airworthiness risks.

- Treating cyber incidents as potential root causes of maintenance errors ensures digital compromises are evaluated for direct safety impacts.

How Information Security Events Impact Aviation Safety

- **Portable Data Loader (PDL) & ARINC 615A Vulnerabilities** Technicians use laptops or Portable Data Loaders to flash Field Loadable Software (FLS) directly into Line Replaceable Units (LRUs) on the aircraft.
 - Security evaluations of ARINC 615A loading protocols revealed that many legacy data loaders do not cryptographically validate file signatures or source media.
 - A technician using an infected maintenance laptop or unauthorized USB drive can inadvertently upload corrupted firmware or altered calibration tables directly to flight-critical avionics.
- **Aerospace Data Breaches & Regulatory Action** Real-world cyber breaches at major aerospace manufacturers and Tier-1 maintenance suppliers, including targeted intrusions at Bombardier and Embraer, proved that malicious actors actively gain access to maintenance IT infrastructure.
 - EASA introduced Part-IS specifically because silent digital corruption presents an immediate airworthiness risk.
- **Supply Chain & Part Traceability Manipulation:** Infiltration of Enterprise Resource Planning (ERP) systems can obscure parts provenance, allowing Suspected Unapproved Parts (SUPs) or life-limited parts with falsified records to enter the assembly chain.

Key Integration Areas: Information Security vs. Safety Management

- **Risk Assessment:** Transition from purely evaluating Confidentiality, Integrity, and Availability for financial or data loss to mapping integrity and availability failures directly to the severity and likelihood of maintenance errors.
- **Hazard Identification:** Expand from monitoring network vulnerabilities and software bugs to tracking cyber-induced operational hazards, such as unavailable digital sign-off tools creating operational time pressure.
- **Occurrence Reporting:** Directly links digital incidents to Regulation (EU) No 376/2014 and Part-145.A.60 reporting pathways, ensuring the 72-hour EASA / National Aviation Authority (NAA) notification clock starts immediately if aircraft airworthiness or safety margins are compromised.
- **Safety & Security Culture:** Extend the "Just Culture" framework to digital errors, ensuring non-punitive reporting for unintentional security mistakes, like plugging in an unknown USB device.

Operationalizing Part-IS within SMS

- **Unified Hazard Register & Risk Matrices:** Translate information security impact metrics into SMS safety risk tolerability matrices. Cyber hazards, such as ransomware locking down technical logs, must undergo a Safety Risk Assessment (SRA) to evaluate downstream effects on aircraft release.
- **Integrated Change Management:** Incorporate Part-IS security impact assessments into the existing SMS Management of Change (MoC) process whenever introducing new digital tools, remote diagnostic devices, or cloud-based maintenance applications.

Strategic Integration of Information Security Management Systems (ISMS) in EASA Part 145 Organisations

Sofema Aviation Considers Key Challenges following the introduction of Regulation (EU) 2023/203. While integrating an Information Security Management System (ISMS) with existing Safety Management Systems (SMS) introduces friction, unmitigated digital vulnerabilities can directly threaten aircraft airworthiness.

Achieving compliance requires a unified governance structure that extends Just Culture principles to cyber incidents, alongside practical measures like MFA & network segregation.

Introduction

Under EASA Regulation (EU) 2023/203 (Part-IS) and Delegated Regulation (EU) 2022/1645, information security is formally codified as a direct operational safety driver of aircraft airworthiness. Unmitigated digital vulnerabilities across ground support equipment, MRO enterprise platforms (e.g., AMOS, Trax), and Portable Data Loaders (PDLs) directly jeopardize Certificate of Release to Service (CRS) integrity and operational safety.

Under EASA Regulation (EU) 2023/203 (Part-IS) and Delegated Regulation (EU) 2022/1645, information security is formally codified as a direct operational safety driver of aircraft airworthiness, mandating the structured elimination of digital vulnerabilities across the Part 145 operational ecosystem.

Core Operational Domain Vulnerabilities

- **Hangar Floor Identity & Access Management:** Prevalence of generic credentials, shared default admin accounts, and open workstations left accessible during fast-paced turnaround maintenance, leading to non-repudiation failures.
- **MRO & CAMO Enterprise Interfaces:** Exploitable inter-organizational APIs (An Application Programming Interface can be defined as a set of rules, which works as an intermediary between two or more applications) and software platforms (e.g., AMOS, Trax) susceptible to data corruption, unauthorized modification of Airworthiness Directive (AD) compliance records, or ransomware lockouts that prevent Certificate of Release to Service (CRS) issuance.
- **Legacy Operational Technology (OT) & Ground Support Tooling:** Automated Test Equipment (ATE), Portable Data Loaders (PDLs), and legacy diagnostic rigs operating on unpatchable or end-of-life operating systems lacking native encryption or security support.
- **Supply Chain & Subcontractor Networks:** Persistent, unmonitored vendor VPN connections, asymmetric cybersecurity maturity across sub-tier repair stations, and software supply chain contamination during Field Loadable Software (FLS) updates or OEM baseline distributions.

Strategic & Technical Mitigations

- **Frictionless Access & Identity Controls:** Eradicate generic logins by enforcing Role-Based Access Control (RBAC) linked directly to individual engineer license authorizations, integrated with low-friction hardware authentication (RFID smart badges, biometrics, or tap-to-login security keys) on the hangar floor.
- **Identity Lifecycle Governance (Onboarding, Transfer, Offboarding):**
 - **Onboarding (Joiners):** Synchronize HR, Compliance, and IT/ISMS workflows to provision access strictly according to Roles.
 - Personal hardware authentication tools (RFID smart badges, security keys) and system accounts are activated only after the completion of mandatory combined SMS/ISMS training, eliminating pre-provisioned or unverified accounts.
 - **Internal Transfer (Movers):** Enforce a strict "least privilege" recalculation to eliminate entitlement creep, instantly revoking system rights.
 - **Offboarding (Leavers):** Execute automated, zero-delay revocation of all digital identities across enterprise platforms (AMOS, Trax), active directories, VPNs, upon employee separation.

- **Data Integrity & Network Hardening:** Implement immutable, timestamped, write-restricted audit logging for all release-to-service actions, combined with API gateway payload inspection, schema validation, and mutual TLS across all MRO/CAMO data flows.
- **Legacy Operational Technology (OT) Defense Controls:** Protect unpatchable diagnostic tools through physical USB/Ethernet port locks, strict application whitelisting, complete internet air-gapping, and isolated subnetwork micro-segmentation.
- **Zero-Trust Supply Chain Controls:** Replace persistent vendor VPN access with time-bound, session-recorded Just-In-Time (JIT) Privileged Access Management (PAM); mandate cryptographic hash verification on air-gapped staging hosts before loading binaries onto aircraft.
- **Unified SMS/ISMS Governance & Extended Just Culture:** Align Safety, Quality, and Information Security Managers under the Accountable Manager, extending non-punitive Just Culture principles to inadvertent cyber slip-ups (e.g., unvetted USB insertion) to preserve internal reporting channels.
- **Mandatory Occurrence Reporting & Compliance Oversight:** Integrate cyber incidents affecting airworthiness data or tooling into the Regulation (EU) No 376/2014 framework, enforcing 72-hour notification to Competent Authorities and Type Certificate Holders (TCH) while incorporating cyber hygiene into routine QA internal and vendor audits.