SOFEMA AVIATION SERVICES

Part-145 – ISMS Process Review Document – PART IS

Governance & Context Establishment Information Security Objectives for the Part-145 Organisation

As an EASA-approved Maintenance Organisation, our ISMS is structured to support the safety, reliability, and compliance of aircraft maintenance operations. Our objectives are aligned with EASA Regulation (EU) 2023/203 and reflect the unique risk profile of maintenance environments.

Part-145 ISMS Objectives:

1. **Protect Confidentiality, Integrity & Availability (CIA)** of maintenance records, component history, and certification documentation.
2. **Ensure Secure Operation of Maintenance Control Systems**, including MRO, ERP, and tool calibration databases.
3. **Control Access to Critical Infrastructure**, including digital tech logs, CRS issuance platforms, and planning dashboards.
4. **Mitigate Risks Arising from Subcontractors & Mobile Teams**, ensuring data security across all interfaces and work locations.
5. **Detect & Respond Effectively to Cyber and Physical Security Incidents**, including unauthorized access, malware intrusion, or compromised systems.
6. **Maintain Compliance** with all applicable regulations including (EU) 2023/203, Part-145, and associated AMC/GM.
7. **Promote Awareness and Competence** in cyber hygiene, secure tool usage, and digital responsibility across all maintenance staff.
8. **Continuously Improve Security Measures** through incident learning, audits, and performance reviews.

1. Protect Confidentiality, Integrity & Availability (CIA) of Maintenance Records, Component History, and Certification Documentation
Context:
In a Part-145 organisation, maintenance records—including component service history, task completion logs, and Certificates of Release to Service (CRS)—form the legal and

technical basis for airworthiness compliance. Any compromise of these records risks aircraft safety, regulatory violations, and legal exposure.

Examples:

- **Confidentiality:** Unauthorized access to component repair reports or digital tech logs via shared logins or poor access controls.
- **Integrity:** Tampering with a signed CRS record could falsely indicate airworthiness.
- **Availability:** System outage during AOG (Aircraft on Ground) scenario preventing access to maintenance documentation and delaying recovery.

Controls Include:

- Role-based access restrictions
- Immutable audit trails on CRS signatures
- High-availability backups and tested recovery protocols

2. Ensure Secure Operation of Maintenance Control Systems, Including MRO, ERP, and Tool Calibration Databases

Context:

Core maintenance operations rely on a range of interconnected digital platforms—from M&E (e.g., AMOS, TRAX) to ERP systems managing parts and workforce, to calibration systems ensuring tools meet safety standards. A cyber breach could cause service disruptions or erroneous maintenance actions.

Examples:

- Manipulated calibration records result in use of unverified torque wrenches
- Malware in ERP disrupts parts provisioning leading to critical maintenance delays

Controls Include:

- Endpoint protection and network segmentation
- Scheduled vulnerability scans and patch management
- MFA (Multi-Factor Authentication) for administrative access

3. Control Access to Critical Infrastructure, Including Digital Tech Logs, CRS Issuance Platforms, and Planning Dashboards

Context:

Part-145 organisations must strictly control who can access, edit, and sign off critical documents such as the tech log and CRS. Unregulated access can compromise safety and legal accountability.

Examples:

- A contractor gains unintended access to planning dashboards, altering maintenance slots
- A junior engineer accesses and signs off a CRS without proper approval or authority

Controls Include:

- Digital signature platforms with role-based access validation
- Automated session timeouts on shared systems in the hangar
- Access revocation procedures upon contract termination

4. Mitigate Risks Arising from Subcontractors & Mobile Teams, Ensuring Data Security Across All Interfaces and Work Locations

Context:

Line maintenance and mobile maintenance teams often operate in remote or third-party-controlled environments (e.g., line stations, hangars abroad). Subcontractors may use their own IT equipment, posing a threat to the ISMS.

Examples:

- A subcontractor using an unprotected laptop connects to internal systems via VPN
- A mobile team fails to encrypt and safely return digital job cards after AOG task completion

Controls Include:

- Enforce BYOD (Bring Your Own Device) policies with endpoint control
- Issue hardened devices for mobile maintenance use
- Subcontractor onboarding with mandatory ISMS briefings and signed NDAs

5. Detect & Respond Effectively to Cyber and Physical Security Incidents, Including Unauthorized Access, Malware Intrusion, or Compromised Systems

Context:

A breach may originate from physical access (e.g., server room entry) or cyber intrusion (e.g., malware in an update file). Fast detection and response are vital to limit disruption and data loss.

Examples:

- Malware enters through a USB used to load task data onto a line station tablet
- Badge cloning grants unauthorized access to a restricted toolroom

Controls Include:

- Security incident playbooks tailored to Part-145 functions
- Physical intrusion detection systems and access logs
- Network monitoring for anomalous behavior or data exfiltration

6. Maintain Compliance with All Applicable Regulations Including (EU) 2023/203, Part-145, and Associated AMC/GM

Context:

The ISMS must integrate seamlessly with the regulatory framework. This includes meeting the cybersecurity requirements outlined in Regulation (EU) 2023/203 and AMC1 IS.I.OR.200(e) regarding ISMS implementation, as well as Part-145 requirements for controlled procedures and safety-critical task performance.

Examples:

- Failure to implement a compliant ISMS may lead to findings during EASA audits
- Lack of evidence for access controls or incident management could violate multiple AMC expectations

Controls Include:

- Documented ISMS Policy linked to Part-145 MOE
- Integration of cybersecurity audits in the QA program
- Risk registers and compliance mapping aligned with AMC1 IS.I.OR.200(b)(4)

7. Promote Awareness and Competence in Cyber Hygiene, Secure Tool Usage, and Digital Responsibility Across All Maintenance Staff

Context:

The human factor is often the weakest link in security. Certifying staff, support engineers, and planning teams must be trained to recognize phishing, use secure practices, and report anomalies.

Examples:

- A technician downloads a fake OEM update infected with spyware
- A staff member sends maintenance records through unsecured email

Controls Include:

- Annual refresher training tied to IT usage policies
- Digital posters in maintenance areas highlighting threats and reporting contacts
- Social engineering tests to reinforce training

8. Continuously Improve Security Measures Through Incident Learning, Audits, and Performance Reviews

Context:

An effective ISMS is not static—it evolves. Learning from real-world incidents, testing recovery plans, and acting on audit findings ensures resilience and relevance.

Examples:

- Post-incident analysis reveals that access revocation processes are too slow
- Annual BCP simulation identifies that CRS platform restoration takes over 6 hours—outside acceptable limits

Controls Include:

- Quarterly ISMS review board meetings
- KPIs and maturity models (e.g., NIST CSF, ISO/IEC 27001 alignment)
- Cross-functional drills (e.g., simulating tool calibration system outage during peak maintenance)

2. ISMS Scope Definition

2.1 Purpose

To define the ISMS boundaries for the Part-145 maintenance organisation in compliance with IS.I.OR.200 and linked to the overall organisational ISMS where applicable.

2.2 Organisational Context

The Part-145 organisation carries out line and base maintenance, component servicing, and engine/APU checks for a range of aircraft types. Work is performed both on-site and at remote line stations. The ISMS supports the secure and uninterrupted flow of maintenance operations and technical communication.

2.3 Scope of the ISMS

Covers all:

- Maintenance planning & execution systems
- Component tracking & tooling calibration platforms
- CRS generation and issuance processes
- Technical documentation access and control
- Remote access by line maintenance teams
- Supplier and subcontractor data exchange
- Mobile and workshop-based device usage
- Maintenance record archiving (digital and paper)

2.4 Interfaces

- **CAMO Interface**: Task cards, forecasts, defect rectification records, reliability findings

Key Data Flows & Security Considerations

The complexity and volume of sensitive data exchanged require rigorous technical, procedural, and governance-level safeguards. By integrating these interface controls into the ISMS structure, a Part-145 organisation ensures both airworthiness and compliance while strengthening its cyber resilience posture.

Would you like this developed further into a dedicated “CAMO Interface Security Control Sheet” or integrated into the ISMS audit checklist format?

1. Task Cards

What They Are:

Digitally or physically transmitted work instructions derived from approved maintenance programs, sometimes customized by the CAMO to include SBs, ADs, or operator-specific procedures.

ISMS Relevance:

- Task cards may contain proprietary data, operational limitations, and safety-critical content.
- If altered, missed, or corrupted, it can result in improper maintenance execution.

Examples of Exposure:

- A cyberattack replaces or deletes a digital task card within the shared MRO platform.
- A subcontractor technician accesses task cards without proper clearance or encryption on a USB drive.
- Manual edits to paper-based task cards introduce undocumented changes not traced back to the CAMO.

Controls:

- Version control and change tracking within the Maintenance Execution System.
- Encrypted task card transmission with access authentication.
- Role-based access control limiting task card download/edit functions.

2. Maintenance Forecasts

Forecasts generated by the CAMO outlining upcoming maintenance checks, component replacements, and inspections. These are shared with the Part-145 organisation for planning, manpower scheduling, and tool readiness.

ISMS Relevance:

- Forecast data includes planning for heavy maintenance (C-checks), critical removals, and service bulletins. An altered or delayed forecast could cause missed airworthiness events.

Examples of Exposure:

- A malicious actor disrupts the XML or API interface delivering forecast data, altering due dates or removing scheduled items.
- An unpatched vulnerability in the CAMO–MRO system interface causes synchronization failures, showing outdated task schedules.

Controls:

- Secure system integration via encrypted APIs (e.g., TLS 1.3 with mutual authentication).

- Periodic reconciliation of forecasts between CAMO and 145 via automated alerts.
- Audit logs for every forecast sync or override operation.

3. Defect Rectification Records

What They Are:

Reports and closing actions for defects raised by flight crew (e.g., via the tech log), identified during scheduled inspections, or flagged through pilot reports (PIREPs).

ISMS Relevance:

- These records are used to verify defect closure and determine ongoing airworthiness status.
- Inaccurate or manipulated defect clearance reports could falsely indicate safety compliance.

Examples of Exposure:

- A malware event causes corruption of closure status flags in the maintenance management system.
- Inadequate access controls allow CAMO personnel to close defect actions meant for Part-145 confirmation.
- Man-in-the-middle attack alters a record showing “open” status as “closed.”

Controls:

- Segregation of duties between CAMO (oversight) and 145 (execution and certification).
- Digital signature verification for every rectification entry.
- End-to-end encryption and validation of digital tech log updates.

4. Reliability Findings

What They Are:

Longitudinal data sent from the Part-145 to the CAMO showing failure trends, component removals, repetitive defects, or unscheduled interventions. This data feeds back into AMP (Approved Maintenance Programme) optimizations.

ISMS Relevance:

- Reliability data integrity is key to predictive maintenance and safety-related escalations.
- False or omitted data undermines the reliability program and CAMO’s ability to justify AMP changes.

Examples of Exposure:

- Excel-based data transmission without encryption or validation creates opportunity for silent corruption.
- A disgruntled insider removes key inputs to hide a pattern of premature component failures.
- Interfacing software incorrectly maps failure codes, distorting MTBUR (Mean Time Between Unscheduled Removals) data.

Controls:

- Digitally signed and time-stamped reliability reports with hash verification.
- Cross-validation between CAMO reliability system and MRO task history.
- Defined input structure using secure templates or machine-readable formats (e.g., JSON/XML via secure API).

Integrated Risk Mitigation Measures for CAMO Interface

Risk Area	Control Strategy
Data tampering or corruption	Audit trails, validation rules, file integrity checks (SHA-256 hashing)
Unintended data access	Role-based access, least privilege enforcement, secure VDI use
Synchronization failure	Scheduled system health checks, retry logic, backup sync logs
Insider manipulation	Segregation of duties, anomaly detection algorithms, strong offboarding process
Vendor/system exploit	Regular interface penetration testing and third-party system patch management

- **OPS Interface**: MEL/CDL status, deferred defect closures, aircraft readiness

The OPS interface is a mission-critical touchpoint in the aircraft dispatch process and a vital control area in the Part-145 ISMS. It demands stringent protection of real-time technical data, harmonized system interaction between maintenance and flight ops, and robust mechanisms to detect and respond to data integrity breaches.

- **MEL/CDL status**, **deferred defect closures**, and **aircraft readiness**
- This interface is a critical coordination point between flight operations and maintenance, carrying significant information security implications under **EASA Regulation (EU) 2023/203**, **Part-145**, and associated AMC/GM materials.

- **2.4 OPS Interface – Detailed Review**
- **Context:**
- The Operations (OPS) department relies on real-time and accurate information from the maintenance environment to make flight release decisions, including managing deferred defects, assessing aircraft dispatch readiness, and applying

MEL/CDL limitations. The integrity, availability, and confidentiality of this data directly affect operational safety, regulatory compliance, and business continuity.

- The flow of information between OPS and Part-145 maintenance is bi-directional and time-critical—particularly during turnarounds, AOG recovery, and MEL/CDL-based dispatch scenarios.

Key Data Flows & Security Considerations

1. MEL/CDL Status

- **What It Is:**
  The Minimum Equipment List (MEL) and Configuration Deviation List (CDL) define the acceptable limitations under which an aircraft may be dispatched with inoperative or missing equipment. These are managed jointly between CAMO/OPS and Part-145.
- **ISMS Relevance:**
- Incorrect MEL/CDL information can result in **unlawful dispatch** or **aircraft grounding**.
- Data must reflect the **current configuration and status** of the aircraft in real time.
- **Examples of Exposure:**
- A shared MEL/CDL dashboard is compromised by ransomware, showing outdated equipment status.
- An unauthorized user alters MEL relief time or deferral expiry dates.
- CDL item is omitted from the flight release documents due to interface data corruption.
- **Controls:**
- MEL/CDL databases integrated with maintenance systems (read-only for OPS, write-controlled by CAMO/145).
- Time-bound digital signatures or auto-expiry for MEL/CDL deferrals.
- Interface security monitoring to detect data synchronization delays or anomalies.

2. Deferred Defect Closures

- **What It Is:**
  Defects identified during operations (e.g., pilot reports, cabin crew log entries) may be deferred under MEL or non-MEL provisions and require confirmation of closure or control actions from Part-145 before flight release.
- **ISMS Relevance:**
- Tampered or falsely closed defects represent **direct threats to flight safety**.
- Incomplete communication between OPS and maintenance can lead to **uncontrolled dispatch**.
- **Examples of Exposure:**

- A digital tech log entry indicating defect closure is intercepted and modified in transit.
- Deferred defect history is inaccessible due to a system outage at the line station.
- The OPS team uses incorrect closure status during aircraft dispatch due to cached data in the EFB.
- **Controls:**
- Encrypted data transfer between tech log and flight planning or EFB systems.
- Real-time defect dashboards with write access restricted to certifying staff only.
- Independent QA validation of closure records linked to Part-145 release.

3. Aircraft Readiness

- **What It Is:**
  A consolidated assessment of an aircraft's technical, legal, and operational state confirming it is fit for dispatch. It encompasses open/closed maintenance items, airworthiness directives, MEL/CDL applicability, and recent defect rectification.
- **ISMS Relevance:**
- Aircraft readiness data underpins go/no-go decisions—**accuracy is paramount**.
- Any delay, manipulation, or unavailability of this information risks operational delays or unsafe release.
- **Examples of Exposure:**
- A misconfigured system shows an aircraft "ready" even though a mandatory maintenance action is overdue.
- A cyberattack renders the readiness dashboard unavailable during pre-departure clearance.
- OPS uses outdated data from a backup system due to poor failover sequencing.
- **Controls:**
- Secure, live interface between the maintenance system and the flight dispatch system.
- System health monitoring and redundancy planning for readiness dashboards.
- Tiered access controls for data entry (145) and consumption (OPS), with audit logs for all transactions.

Integrated Risk Mitigation Measures for the OPS Interface

Risk Category	**Mitigation Measures**
Inaccurate MEL/CDL data	Enforced time-bound entries, alerting for deferral expiry, cryptographic validation
Deferred defect spoofing	Strong user authentication, tamper-evident closure workflow

Readiness data integrity	System uptime monitoring, fallback validation process with QC oversight
Unauthorized access	Least privilege access model for OPS staff, regular privilege reviews
System outage impact	Redundant system architectures and real-time replication

ISMS Requirements Alignment

- **IS.I.OR.200(e):** Ensures cybersecurity controls protect MEL/CDL and readiness data at rest, in use, and in transit.
- **IS.I.OR.220:** Requires incident detection (e.g., tampering, availability outage) be logged, classified, and responded to with urgency if affecting operational status.

- **IT Interface**: Access control, software support, network management

1. Access Control

What It Is:

Access control defines who is allowed to access which systems, data sets, and functions within the Part-145 environment—typically enforced by IT via identity management, credentials, and authentication mechanisms.

ISMS Relevance:

- Access must be **role-based**, time-limited, and strictly monitored—especially for certifying staff, planning engineers, and external vendors.
- Improper access rights or dormant accounts can become entry points for **privilege escalation**, **data tampering**, or **unlawful certification**.

Examples of Exposure:

- A recently terminated subcontractor retains access to the M&E system for two weeks post-departure.
- Shared user accounts are used in hangars, making it impossible to trace CRS entries to individual certifying staff.
- MFA is disabled during system maintenance and not reactivated, exposing systems to credential-based attacks.

Controls:

- Centralized Identity and Access Management (IAM) with role-based access (RBAC) aligned to Part-145 authorisations.
- Enforced password policy, MFA, and session timeout protocols.
- Automated access revocation on contract termination and HR-driven access provisioning workflows.

2. Software Support

What It Is:

This involves the ongoing maintenance, patching, and upgrading of applications used by the Part-145 team, including the M&E system, calibration software, task card libraries, and document control systems.

ISMS Relevance:

- Unpatched vulnerabilities can be exploited by attackers to gain lateral access across operational domains.
- Unsupported legacy systems pose both security and operational risk due to incompatibility with secure infrastructure.

Examples of Exposure:

- A planning dashboard runs on a deprecated browser, exposing the interface to cross-site scripting (XSS).
- A mobile application used by line maintenance staff is no longer receiving vendor updates and becomes a malware risk.
- Maintenance records are stored in an Excel-based system without encryption or access controls.

Controls:

- Maintain a **Software Asset Inventory** with update status and end-of-life dates.
- Implement **Patch Management SOPs** aligned to system criticality and supplier notifications.
- Isolate legacy systems via network segmentation and limit them to read-only access where applicable.

3. Network Management

What It Is:

The configuration and control of the network infrastructure used to transport data between Part-145 systems (e.g., workstations, servers, mobile devices) and external domains (e.g., CAMO, OCC, external suppliers).

ISMS Relevance:

- Network security forms the first layer of defense against external threats.
- Poor segmentation or lack of monitoring can allow **undetected intrusions**, **data exfiltration**, or **service disruption**.

Examples of Exposure:

- A technician connects a personal device to a corporate Wi-Fi network in a hangar and unintentionally introduces malware.
- A misconfigured firewall allows inbound remote access to the MRO system from unsecured IP ranges.
- No monitoring exists for lateral movement within the VLAN supporting the CRS platform.

Controls:

- Enforce **network segmentation** between administrative, operational, and guest domains.
- Deploy **Intrusion Detection/Prevention Systems (IDS/IPS)** and log all internal and external traffic patterns.
- Restrict external network access (e.g., VPN, remote desktops) with geofencing and scheduled access controls.

Integrated Risk Mitigation Measures for IT Interface

Risk Category	Mitigation Strategy
Unauthorized access	IAM with least privilege, MFA, and timely revocation of user rights
Exploitable legacy systems	Isolation, restricted access, and software lifecycle tracking
Malware propagation	Endpoint Detection & Response (EDR), USB control policies, user behavior analytics
Unsecured remote access	Hardened VPNs, firewall rules, zero-trust network access policies
Monitoring gaps	Centralized SIEM logging and anomaly detection

ISMS Compliance Integration

- **AMC1 IS.I.OR.200(e)(2):** Emphasizes appropriate safeguards for identity and access management systems—directly addressed by IAM and role-based controls.
- **AMC1 IS.I.OR.220:** Requires detection and response for IT-originated incidents—fulfilled by logging, IDS/IPS deployment, and incident escalation SOPs.

- **Subcontractor Interface**: Secure task delivery, certification return, audit sharing

This interface is particularly sensitive from a cybersecurity perspective due to outsourced operational execution, potential IT segregation gaps, and reduced direct control over non-staff actors. Regulation (EU) 2023/203, as well as EASA Part-145.A.70 and AMC/GM, require that subcontracted activities be appropriately controlled and traceable within the approved system.

2.4 Subcontractor Interface – Detailed Review

Subcontractors are frequently used in line maintenance, heavy base maintenance, NDT (Non-Destructive Testing), engine support, and logistics handling. These entities may operate onsite, remotely, or across international locations—making cybersecurity and information assurance both complex and critical.

This interface governs the digital and procedural exchange of safety-critical information—such as task assignments, component handling records, and CRS documentation—with third-party organisations. If mishandled, it could expose the Part-145 organisation to regulatory violations, airworthiness risks, and data leaks.

Key Functional Areas & Security Considerations

1. Secure Task Delivery
What It Is:
The transmission of scheduled work packages, maintenance instructions (e.g. task cards), or engineering orders to subcontractors.
ISMS Relevance:

- Data must be securely transmitted, traceable, and only accessible to authorized personnel.
- Modifications by subcontractors must be controlled and logged, ensuring integrity of maintenance instructions.

Examples of Exposure:

- A subcontractor receives maintenance instructions via unencrypted email, exposing task data to interception.
- A shared file transfer link is accidentally sent to an unrelated organisation.
- Paper-based task cards are lost during transit to a remote line station.

Controls:

- Use Digital Rights Management (DRM) or encrypted SharePoint/portal access with time-based expiry.
- Log all task card downloads and user access sessions.
- Apply watermarks and version control to prevent unofficial modifications.

2. Certification Return
The process by which subcontractors return documentation certifying work performed (e.g. CRS, Form 1, work orders), which the primary Part-145 organisation must review and integrate into the aircraft's technical records.
ISMS Relevance:

- Certification documents represent legal attestation of airworthiness-related work—integrity and authenticity are critical.
- Digital transmission methods must prevent forgery, tampering, or loss.

Examples of Exposure:

- A subcontractor uploads a scanned CRS PDF to a shared folder that is accidentally accessed by a third party.
- The CRS is submitted without a digital signature, allowing post-submission editing.
- Delays or corruption in the file transmission result in the wrong CRS being uploaded to the aircraft record.

Controls:

- Require digitally signed and hash-verified documents (e.g. PKI-based digital signature with embedded timestamp).
- Implement document validation workflow before upload into MRO system.
- Mandate secure submission channels (SFTP, corporate cloud with MFA).

3. Audit Sharing

What It Is:

The exchange of security, quality, and compliance audit data between the Part-145 organisation and subcontractors, either as part of due diligence, regulatory compliance, or incident investigations.

ISMS Relevance:

- Audit reports contain sensitive findings, process weaknesses, and sometimes personal data—making confidentiality and traceability essential.
- Uncontrolled access to audit results may expose the organisation to reputational risk or regulatory scrutiny.

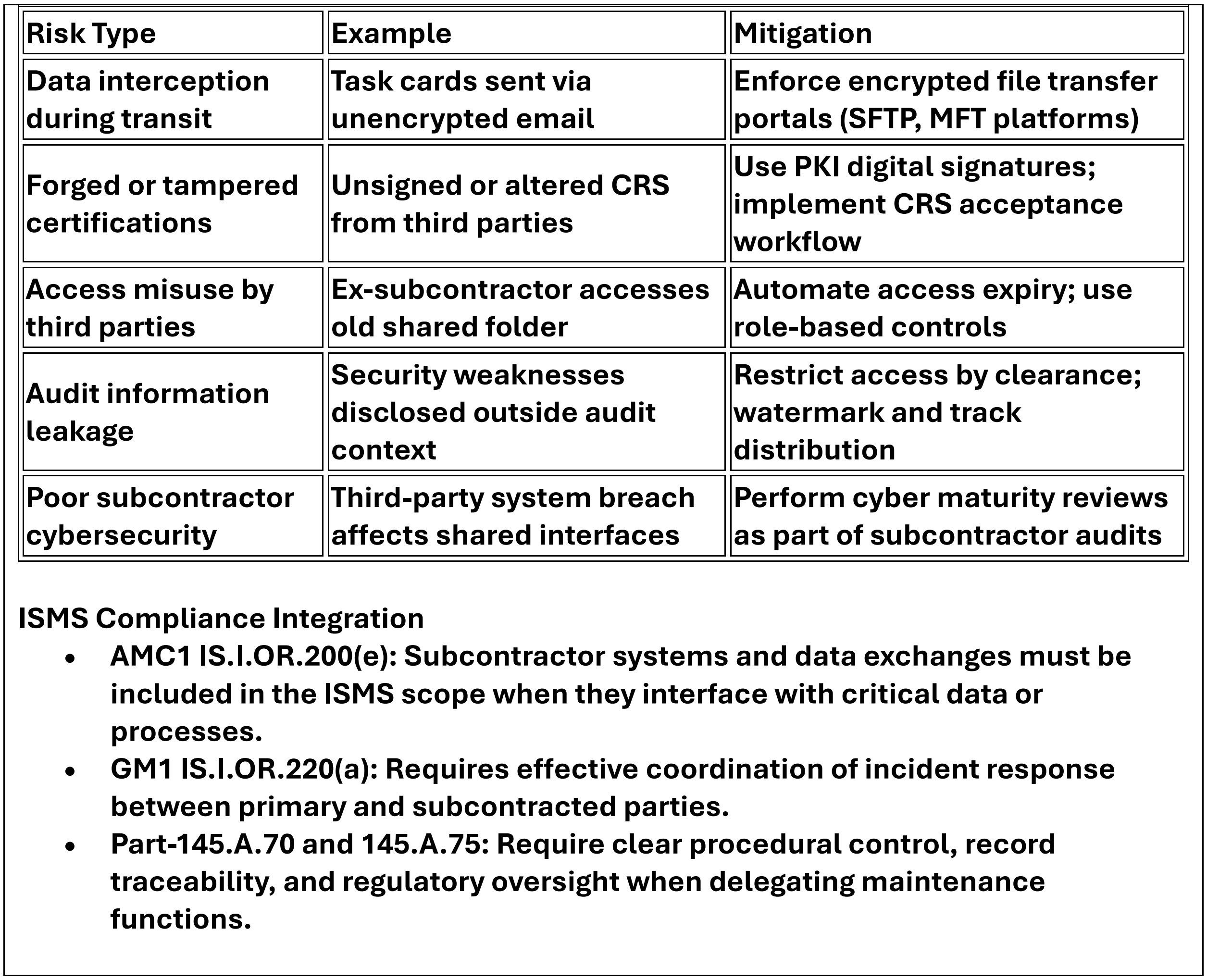
Examples of Exposure:

- An audit report highlighting an IT vulnerability is shared via email and later leaked externally.
- Subcontractors refuse to share requested audit reports or provide redacted versions with integrity issues.
- Discrepant audit logs result from incompatible digital systems, making incident investigations unreliable.

Controls:

- Establish Data Sharing Agreements (DSA) with subcontractors that define audit report ownership, use, and transmission format.
- Use secure audit portals with access logs, download history, and classification marking.
- Integrate audit sharing into contractual obligations, including periodic cyber-readiness assessments.

Cross-Cutting Security Risks and Mitigation Strategies



Risk Type	Example	Mitigation
Data interception during transit	Task cards sent via unencrypted email	Enforce encrypted file transfer portals (SFTP, MFT platforms)
Forged or tampered certifications	Unsigned or altered CRS from third parties	Use PKI digital signatures; implement CRS acceptance workflow
Access misuse by third parties	Ex-subcontractor accesses old shared folder	Automate access expiry; use role-based controls
Audit information leakage	Security weaknesses disclosed outside audit context	Restrict access by clearance; watermark and track distribution
Poor subcontractor cybersecurity	Third-party system breach affects shared interfaces	Perform cyber maturity reviews as part of subcontractor audits

ISMS Compliance Integration

- **AMC1 IS.I.OR.200(e): Subcontractor systems and data exchanges must be included in the ISMS scope when they interface with critical data or processes.**
- **GM1 IS.I.OR.220(a): Requires effective coordination of incident response between primary and subcontracted parties.**
- **Part-145.A.70 and 145.A.75: Require clear procedural control, record traceability, and regulatory oversight when delegating maintenance functions.**

3. Policy Linkage to Corporate ISMS

A clear and traceable policy alignment exists between the Part-145 ISMS and the overarching organisational ISMS.

- **Focal Point**: Part-145 Post Holder (Maintenance Manager or QA)
- **Reports to**: Chief Information Security Officer (CISO)
- **Documents Aligned**: ISMS-POL-001, 145-PRO-IS01 (Security Event Reporting), 145-PRO-IS02 (Access Control Management)

---

4. Stakeholder Mapping

Domain	Stakeholders
Internal	Maintenance Planners, Certifying Staff, QA Inspectors, Stores Personnel
External	CAMO Engineers, IT Vendors, Component Suppliers, Subcontracted AMOs
Systems Support	M&E Software Provider, Network Admin, Backup & Recovery Support Team

---

5. Asset Mapping

a. Digital Assets

- M&E System (e.g. AMOS, TRAX)
- Tooling & Calibration Database
- Work Order & Job Card Systems
- Component Traceability & AD/SB compliance tools
- CRS Generation Portals
- CCTV & Keycard Access Control Logs

1. M&E System (e.g., AMOS, TRAX, OASES)
Function:
These platforms form the digital backbone of aircraft maintenance execution. They manage planning, task execution, parts consumption, defect reporting, and maintenance record storage.
ISMS Relevance:

- **Stores legally binding airworthiness records**
- **Interfaces with CAMO and planning teams**
- **High-value target for ransomware or privilege escalation**

Examples of Exposure:

- **SQL injection vulnerability in TRAX exploited to access user credential database**
- **Insider misuse—engineer with elevated rights deletes scheduled tasks and modifies work status**

- Lack of logging prevents root cause investigation after suspicious record changes

Security Controls:

- Role-Based Access Control (RBAC)
- Encryption at rest and in transit
- Immutable audit trails for changes and user actions
- Integration with Identity Access Management (IAM) and MFA

2. Tooling & Calibration Database

Function:

Maintains status, calibration history, and next due dates of all tools and equipment used in maintenance. Often includes torque wrenches, pressure gauges, and avionics testing devices.

ISMS Relevance:

- Uncalibrated tools directly compromise aircraft safety and regulatory compliance
- Data integrity ensures that tools are serviceable and traceable at all times

Examples of Exposure:

- Unauthorized edit of calibration status leading to unverified tool use
- Database corruption causes loss of tool due-dates, resulting in grounded aircraft
- Cloud-based calibration system hacked, modifying tolerance thresholds

Security Controls:

- Access logs and user tracking for calibration status changes
- Read-only access for end-users; admin changes require justification
- Scheduled backups and reconciliation with physical calibration labels

3. Work Order & Job Card Systems

Function:

Digitally delivers task cards, work packs, and engineering work instructions. These may include aircraft-specific procedures, SB/AD applicability, and configuration data.

ISMS Relevance:

- Work orders guide safety-critical maintenance; tampering can lead to invalid tasks or missed steps
- Real-time task data is used for shift handovers, audits, and final CRS preparation

Examples of Exposure:

- Delay or denial of service attack on job card portal during overnight hangar shift

- A duplicated job card is accidentally completed twice, resulting in invalid maintenance records
- A phishing attack delivers fake work order link mimicking the official platform

Security Controls:

- Use of authenticated portals with data encryption
- Time-stamped, version-controlled job card delivery
- API integrity checks for CAMO-to-145 data syncing

4. Component Traceability & AD/SB Compliance Tools

Function:

Systems that track the movement, installation, and removal of aircraft components—including life-limited parts, serialized inventory, and regulatory compliance with Airworthiness Directives (ADs) and Service Bulletins (SBs).

ISMS Relevance:

- Traceability and AD compliance are legal mandates
- Data loss or manipulation may allow installation of non-compliant or time-expired parts

Examples of Exposure:

- Component swapped during maintenance but traceability system not updated due to outage
- Remote attacker modifies AD status to "not applicable," allowing flight with unaddressed directive
- Discrepancies in SB applicability status between CAMO system and 145 database

Security Controls:

- Daily synchronization and hash validation of component records
- Digital signatures for part movements and removals
- Restricted editing access for AD/SB applicability and closing actions

5. CRS Generation Portals

Function:

Digital systems used by certifying staff to issue Certificates of Release to Service (CRS) following task completion. These are considered legally binding airworthiness attestations.

ISMS Relevance:

- CRS records must be accurate, tamper-proof, and traceable to the responsible licensed engineer
- A compromised CRS portal can falsely indicate airworthiness or hide outstanding defects

Examples of Exposure:

- CRS issued from a compromised device with a spoofed user session

- **Insecure login allows impersonation of B1 or B2 certifying staff**
- **CRS file corrupted during transfer to archive server**

Security Controls:

- **CRS issued only via MFA-protected sessions with identity tracking**
- **Timestamp and geolocation metadata embedded in CRS records**
- **Enforced document integrity using hash comparison and PDF locking**

6. CCTV & Keycard Access Control Logs

Function:

Security systems that log and monitor physical access to maintenance areas, tool stores, calibration labs, and server rooms. These logs are critical for incident forensics and access validation.

ISMS Relevance:

- **Physical security is a core component of digital asset protection**
- **Access logs provide accountability for events (e.g., tampering, data theft)**

Examples of Exposure:

- **Badge cloning grants unauthorized access to the tool crib, leading to tool disappearance**
- **Logs overwritten before an incident investigation is completed**
- **Networked CCTV feed is hijacked or turned off by malware during sabotage**

Security Controls:

- **Tamper-resistant DVR systems with restricted access**
- **Integration with employee access logs and shift rosters**
- **Automated alerts for unauthorized or out-of-hours entry attempts**

b. Physical Assets

- Tech log hardcopies
- Printed task cards & CRS
- Laptops, tablets, mobile devices used at hangars
- Encrypted USBs for file exchange with line stations

1. M&E System (e.g., AMOS, TRAX, OASES)

Function:

These platforms form the digital backbone of aircraft maintenance execution. They manage planning, task execution, parts consumption, defect reporting, and maintenance record storage.

ISMS Relevance:

- Stores legally binding airworthiness records
- Interfaces with CAMO and planning teams
- High-value target for ransomware or privilege escalation

Examples of Exposure:

- SQL injection vulnerability in TRAX exploited to access user credential database
- Insider misuse—engineer with elevated rights deletes scheduled tasks and modifies work status
- Lack of logging prevents root cause investigation after suspicious record changes

Security Controls:

- Role-Based Access Control (RBAC)
- Encryption at rest and in transit
- Immutable audit trails for changes and user actions
- Integration with Identity Access Management (IAM) and MFA

2. Tooling & Calibration Database

Function:

Maintains status, calibration history, and next due dates of all tools and equipment used in maintenance. Often includes torque wrenches, pressure gauges, and avionics testing devices.

ISMS Relevance:

- Uncalibrated tools directly compromise aircraft safety and regulatory compliance
- Data integrity ensures that tools are serviceable and traceable at all times

Examples of Exposure:

- Unauthorized edit of calibration status leading to unverified tool use
- Database corruption causes loss of tool due-dates, resulting in grounded aircraft
- Cloud-based calibration system hacked, modifying tolerance thresholds

Security Controls:

- Access logs and user tracking for calibration status changes
- Read-only access for end-users; admin changes require justification
- Scheduled backups and reconciliation with physical calibration labels

3. Work Order & Job Card Systems

Function:

Digitally delivers task cards, work packs, and engineering work instructions. These may include aircraft-specific procedures, SB/AD applicability, and configuration data.

ISMS Relevance:

- Work orders guide safety-critical maintenance; tampering can lead to invalid tasks or missed steps
- Real-time task data is used for shift handovers, audits, and final CRS preparation

Examples of Exposure:

- Delay or denial of service attack on job card portal during overnight hangar shift
- A duplicated job card is accidentally completed twice, resulting in invalid maintenance records
- A phishing attack delivers fake work order link mimicking the official platform

Security Controls:

- Use of authenticated portals with data encryption
- Time-stamped, version-controlled job card delivery
- API integrity checks for CAMO-to-145 data syncing

4. Component Traceability & AD/SB Compliance Tools

Function:

Systems that track the movement, installation, and removal of aircraft components—including life-limited parts, serialized inventory, and regulatory compliance with Airworthiness Directives (ADs) and Service Bulletins (SBs).

ISMS Relevance:

- Traceability and AD compliance are **legal mandates**
- Data loss or manipulation may allow installation of non-compliant or time-expired parts

Examples of Exposure:

- Component swapped during maintenance but traceability system not updated due to outage
- Remote attacker modifies AD status to “not applicable,” allowing flight with unaddressed directive
- Discrepancies in SB applicability status between CAMO system and 145 database

Security Controls:

- Daily synchronization and hash validation of component records
- Digital signatures for part movements and removals
- Restricted editing access for AD/SB applicability and closing actions

5. CRS Generation Portals

Function:

Digital systems used by certifying staff to issue Certificates of Release to Service (CRS) following task completion. These are considered **legally binding airworthiness attestations**.

ISMS Relevance:

- CRS records must be accurate, tamper-proof, and traceable to the responsible licensed engineer
- A compromised CRS portal can falsely indicate airworthiness or hide outstanding defects

Examples of Exposure:

- CRS issued from a compromised device with a spoofed user session

- Insecure login allows impersonation of B1 or B2 certifying staff
- CRS file corrupted during transfer to archive server

Security Controls:

- CRS issued only via MFA-protected sessions with identity tracking
- Timestamp and geolocation metadata embedded in CRS records
- Enforced document integrity using hash comparison and PDF locking

6. CCTV & Keycard Access Control Logs

Function:

Security systems that log and monitor physical access to maintenance areas, tool stores, calibration labs, and server rooms. These logs are critical for **incident forensics** and access validation.

ISMS Relevance:

- Physical security is a core component of digital asset protection
- Access logs provide accountability for events (e.g., tampering, data theft)

Examples of Exposure:

- Badge cloning grants unauthorized access to the tool crib, leading to tool disappearance
- Logs overwritten before an incident investigation is completed
- Networked CCTV feed is hijacked or turned off by malware during sabotage

Security Controls:

- Tamper-resistant DVR systems with restricted access
- Integration with employee access logs and shift rosters
- Automated alerts for unauthorized or out-of-hours entry attempts

6. Risk Identification Summary (See end of document)

Typical Risks in the 145 Domain include:

- Shared access to terminals used by multiple certifying staff without proper session isolation
- Poor endpoint security on field maintenance devices
- Malware introduction through infected USBs during hangar work
- Subcontractor access via VPN using non-corporate devices
- Uncontrolled use of mobile apps to log CRS or maintenance task status
- Delay in revocation of access for expired contractor credentials

7. Threat & Vulnerability Landscape

Source	Example
Insiders	Misuse of access to modify CRS post-event
External Attackers	Phishing targeting certifying staff or engineers
Legacy Systems	End-of-life calibration software or unsupported tablet OS
Misconfigurations	Work package storage on shared, publicly accessible drives
Third Party	Inadequate endpoint protection from contracted AMO or tooling provider

1. Insider Threats

Authorized personnel who misuse their access—intentionally or accidentally—to harm system integrity, airworthiness records, or operational safety.

Examples:

- A licensed engineer with extended access modifies a **Certificate of Release to Service (CRS)** after aircraft dispatch to conceal an incomplete task.
- Generic logins used in line stations prevent accountability, allowing **unauthorized system changes** without traceability.
- A staff member copies aircraft status reports onto a personal **USB stick**, later lost in an unsecured location.

Mitigation Measures:

- Role-Based Access Control (RBAC) with strict permissions
- Immutable audit logs for all data and certification entries
- Insider threat detection via user behavior analytics
- Personal credentials only; no shared accounts

2. External Attackers

Definition:

Unauthorized actors—cybercriminals, hacktivists, or state-backed intruders—who exploit vulnerabilities for sabotage, financial gain, or data theft.

Examples:

- **Phishing emails** mimic IT notifications to trick certifying staff into entering credentials into fake M&E login portals.
- A ransomware attack triggered by an infected attachment locks access to **maintenance history and planning systems**, grounding the fleet.
- **Spoofed helpdesk calls** convince staff to disable endpoint protection, opening the system to external remote control.

Mitigation Measures:

- Email and phishing training, secure DNS and email gateways
- Endpoint Detection and Response (EDR) tools
- Multi-Factor Authentication (MFA) and login attempt throttling
- Incident Response Plan with ransomware-specific playbooks

3. Legacy Systems

Definition:

Obsolete or end-of-life systems no longer supported by vendors and thus lacking critical security patches or compatibility with modern controls.

Examples:

- Calibration software running on **Windows XP** becomes a **backdoor vector** due to unpatched vulnerabilities.
- Tablets on **Android 7** used for task completion lack encryption or certificate support, exposing user data.
- Old planning software is incompatible with antivirus and firewall systems, prompting users to **disable security tools**.

Mitigation Measures:

- Isolation (VLAN or offline) of legacy systems
- Upgrade and lifecycle plans with budgeted timelines
- Compensating controls (e.g., monitored proxy gateways)
- Limited access and restricted use policies

4. Misconfigurations

Definition:

Incorrect system, network, or software setups that expose services, weaken access control, or allow unintended data access.

Examples:

- A planner saves a **work package on a shared network drive** accessible by the entire company—no authentication required.
- Remote desktop access left **open to the internet** with default credentials allows external login attempts.
- Backups configured without verifying database integrity miss critical files, **invalidating disaster recovery**.

Mitigation Measures:

- Secure configuration baselines and review audits
- Principle of Least Privilege for file and system access
- Network segmentation and firewall hardening
- Scheduled recovery testing and configuration validation

5. Third Party Threats

Definition:

Risks introduced by suppliers, subcontractors, tool providers, or remote AMO partners with system or data access.

Examples:

- A subcontracted AMO accesses the M&E system using **an unprotected laptop** infected with malware—resulting in system compromise.
- Tool vendor delivers calibration data via **unencrypted USB**, which also carries auto-executing malicious code.
- Line maintenance partner emails CRS PDFs without password protection or secure transfer—creating a **data interception risk**.

Mitigation Measures:

- Cybersecurity requirements included in contracts and SLAs
- Third-party access reviews and endpoint verification
- Data exchange only via secure platforms (e.g., SFTP, portals)
- Supplier cyber maturity assessments and audit integration

Conclusion: Integrated ISMS Risk Strategy

An effective ISMS for a Part-145 organisation must anticipate and defend against both **direct and indirect threats**. This includes:

- Internal misuse and negligence
- External, targeted cyberattacks
- Technical debt from legacy assets
- Configuration weaknesses and human error
- Third-party risks across supply and maintenance chains

8. ISMS Control Framework (Part 145 Specific Focus)

- **RBAC Enforcement**: Certifying staff roles limited to their A/C types & approvals
- **CRS Audit Trails**: Digital logs of signature events
- **Access Control Logs**: Secure logins on shared tools

- **Secure Work Package Transmission**: DRM or protected SharePoint for task card transfer
- **MFA Implementation**: For all high-risk or remote system access
- **Backup & Restore**: Job cards, defect closure records backed up and version-controlled

1. RBAC Enforcement (Role-Based Access Control)
Control:
Access rights are granted strictly based on job roles, license types, and approved aircraft categories.
Part-145 Focus:

- Certifying staff should only be able to issue CRS or perform sign-offs on aircraft types for which they are **authorized under their license and organizational approval**.
- Maintenance planners, quality staff, and administrative users must have **segregated permissions** based on least-privilege principles.

Examples of Implementation:

- A B1 engineer is blocked from accessing B2 avionics task cards or sign-off screens for which they have no authorization.
- Line maintenance staff may view open defects but cannot close them or modify historical job records.
- Temporary access is granted to subcontractors with **automated expiry after job completion**.

Mitigation of Risk:

- Prevents unauthorized CRS issuance or access to controlled documents.
- Minimizes insider threat and human error exposure.
- Supports clean audit trails and reduces privilege creep.

2. CRS Audit Trails
Control:
Every Certificate of Release to Service (CRS) issued must be digitally logged, capturing the user ID, timestamp, aircraft registration, work package ID, and geolocation if remote.
Part-145 Focus:

- CRS is a **legal statement of airworthiness**. Post-signature tampering or unauthorised overrides must be impossible or fully traceable.
- Audit trails must be immutable, secure, and accessible to QA for internal or regulatory audits.

Examples of Implementation:

- A certifying engineer signs off a base maintenance work pack; the system records the event with time, aircraft, workstation ID, and digital signature.
- If an attempt is made to edit a signed CRS entry, the system **blocks the action** or creates a flagged exception entry.

Mitigation of Risk:

- Ensures accountability and authenticity of sign-off events.
- Supports root cause analysis during investigations or occurrence reporting.
- Demonstrates full compliance with Part-145.A.50 and associated record-keeping obligations.

3. Access Control Logs (Secure Logins on Shared Tools)

Control:

Systems that control tooling access, calibration stations, or hangar terminals must require individual login credentials and track access events.

Part-145 Focus:

- Shared tooling (e.g. borescope workstations or weighing systems) should **not allow unauthenticated or group access**.
- Access must be monitored and integrated into overall ISMS logging.

Examples of Implementation:

- Calibration room access terminals require login cards; each use is recorded with employee ID and time.
- Maintenance laptops authenticate users via Active Directory and log every session to a central SIEM.

Mitigation of Risk:

- Enhances traceability for tooling misuse or manipulation of calibration settings.
- Provides reliable forensic data in the event of a process deviation or incident.

4. Secure Work Package Transmission

Control:

Digital Rights Management (DRM) or protected document-sharing platforms (e.g. SharePoint with version control) must be used for transferring task cards, job packs, and engineering orders.

Part-145 Focus:

- Particularly critical for line stations, subcontractors, and remote maintenance teams where connectivity is variable.
- Paperless workflows increase speed but also raise exposure to **data interception or modification** if not secured.

Examples of Implementation:

- Task cards are uploaded to a SharePoint site with read-only access, expiry timestamps, and download logging.

- Work packs include QR codes linking back to a central validated version, ensuring field engineers cannot mistakenly use outdated documents.

Mitigation of Risk:

- Prevents uncontrolled duplication or unapproved modifications.
- Tracks document access and sharing for audit purposes.
- Enables version enforcement and traceability.

5. MFA Implementation (Multi-Factor Authentication)

Control:

All high-risk systems—such as CRS portals, M&E system admin consoles, remote maintenance access, and document repositories—must require multi-factor authentication.

Part-145 Focus:

- Prevents unauthorized access from compromised credentials, particularly in remote or mobile work environments.
- Should be enforced for VPNs, critical planning tools, and mobile access points.

Examples of Implementation:

- Certifying engineers use an **authenticator app or smart card** in addition to their password to log into AMOS or TRAX.
- Remote access to job data from an outstation requires both biometric login and a one-time passcode.

Mitigation of Risk:

- Significantly reduces the risk of phishing and credential-based attacks.
- Enforces identity assurance at critical decision points.

6. Backup & Restore (Job Cards and Defect Records)

Control:

All essential maintenance records—job cards, defect closure reports, and part movements—must be regularly backed up and subject to **version-controlled restoration capability**.

Part-145 Focus:

- Ensures availability of airworthiness data in case of system failure, cyberattack, or accidental deletion.
- Must include both structured data (in SQL databases) and unstructured files (PDFs, scanned documents).

Examples of Implementation:

- Daily backups of all open and closed work orders, with **encrypted off-site replication**.
- Backup retention policy ensuring 36-month record availability to meet EASA record-keeping requirements.

- Restoration drills verifying full recovery of a randomly selected work pack within SLA timelines.

Mitigation of Risk:

- Enables operational continuity in the event of cyber or infrastructure disruption.
- Avoids regulatory non-compliance due to lost maintenance records.
- Supports litigation defense and insurer audits by ensuring data authenticity and availability.

9. Incident Detection and Recovery

- **Severity Classification**: Tailored to maintenance-criticality (e.g., lost access to CRS portal = Severity 1)
- **Playbooks**: Response plans for malware infection, outage of M&E, or vendor platform failure
- **Communication Tools**: Emergency MS Teams, VoIP, SMS alerting
- **BCP Simulations**: AOG scenario simulations, base maintenance disruption drills

1. Severity Classification

Definition:

Incidents must be **graded according to their impact** on safety-critical processes, system availability, and regulatory obligations. The classification system enables timely escalation and resource allocation.

Part-145 Specific Approach:

- Classifications should be **tied to maintenance-criticality**, not just generic IT parameters.

Examples:

- **Severity 1** – Loss of access to CRS portal: Prevents legal release of aircraft; immediate threat to operational continuity.
- **Severity 2** – Malware detected on a non-critical planning workstation: Contained risk, affects planning team, not immediate flight risk.
- **Severity 3** – Delay in uploading updated task cards for a future maintenance slot: Low urgency, operational workaround possible.

Mitigation Benefits:

- Prevents over/underreaction to incidents
- Facilitates structured escalation aligned with airworthiness impact
- Enables data-driven prioritization of incident resolution

2. Playbooks (Standardized Response Plans)

Definition:

Documented, repeatable procedures that guide teams in responding to specific incident types, ensuring **fast, compliant, and coordinated response** across departments.

Part-145 Use Cases:

- Tailored playbooks must exist for incidents involving **M&E systems**, subcontractor breaches, and loss of operational data.

Examples:

- **Malware Infection:**
  Isolation of infected hangar workstation, notification to IT Security, forensic image capture, validation of no impact on M&E database.
- **M&E System Outage:**
  Switch to paper-based task documentation, activate redundant offline task cards, QA monitoring for all manual sign-offs during the downtime.
- **Vendor Platform Failure (e.g., outsourced calibration data portal):**
  Trigger SLA clause, escalate to vendor CISO, activate manual calibration record retrieval from backup or redundant provider.

Mitigation Benefits:

- Reduces mean time to detect/respond (MTTD/MTTR)
- Limits operational damage and regulatory exposure
- Ensures continuity even in outsourced service failures

3. Communication Tools

Definition:

Reliable, redundant channels for intra- and inter-team coordination during incident response, especially when primary systems are compromised.

Part-145 Priorities:

- Must support **multi-site coordination** (base, line, and third-party stations) and ensure **traceable, real-time communication**.

Examples:

- **Microsoft Teams (Emergency Channels):**
  Dedicated chat for Crisis Management Team (CMT) with restricted access, logs preserved for post-incident analysis.
- **VoIP with Failover:**
  Secondary voice communications platform used when corporate PBX is affected by outage or cyberattack.
- **SMS Push Notifications:**
  Emergency alerts sent to key personnel, including certifying engineers and QA staff, in case of M&E compromise or credential breach.

Mitigation Benefits:

- Prevents confusion and delay in response during primary system failure

- Maintains operational awareness across distributed teams
- Enhances regulatory defensibility through documented traceability

4. Business Continuity Plan (BCP) Simulations
Definition:
Structured, periodic exercises that test the effectiveness and readiness of the BCP under realistic scenarios. Should simulate cyber and operational disruptions with safety impact.

Part-145 Maintenance-Driven Scenarios:

- Focus on how **airworthiness, compliance, and continuity of maintenance delivery** are protected under stress.

Examples:

- **AOG Scenario:**
  Simulate ransomware disabling access to AMOS at a line station during unscheduled defect rectification. Team must execute offline workflows and complete CRS using pre-approved manual templates.
- **Base Maintenance Disruption Drill:**
  Simulate fire alarm or network blackout during C-check. Evaluate staff readiness to continue operations using offline job packs, manual inventory updates, and ERP delay compensation.
- **Third-Party Data Breach Exercise:**
  Simulate leak of component service history via compromised subcontractor interface. Exercise internal reporting, subcontractor notification, and legal response.

Mitigation Benefits:

- Validates effectiveness of fallbacks and workarounds
- Builds team confidence and role clarity under stress
- Reveals gaps in response plans, documentation, or training

10. Training & Awareness

- Job-role specific security induction
- Annual refresher covering:
  - Secure handling of digital tech logs
  - Safe usage of mobile platforms
  - Threat recognition (phishing, social engineering)

10. Training & Awareness (Part-145 Specific Focus)

In a Part-145 environment, human factors are a **leading cause of cybersecurity incidents**, whether through misjudgment, negligence, or social engineering. A well-structured, role-specific training and awareness program significantly reduces these risks and supports overall airworthiness by protecting data integrity and system availability.

1. Job-Role Specific Security Induction

Definition:

All new personnel must receive an ISMS-focused induction tailored to their **job responsibilities, system access, and operational context**. This ensures they understand their specific cyber obligations from day one.

Examples:

- **Certifying Staff:**
  Induction includes instruction on **secure CRS completion**, protection of credentials, and policies for using personal devices in hangars or at line stations.
- **Planners:**
  Focus on protecting **maintenance forecasts, task cards**, and sensitive maintenance program data; guidance on **secure document sharing** and calendar integrations.
- **Tooling & Calibration Technicians:**
  Emphasis on using only **authorized calibration platforms**, safe USB practices, and tracking tool traceability data securely.
- **Subcontractors:**
  Given a **contractor-specific briefing**, covering access control policies, endpoint protection requirements, and incident reporting protocols.

Benefit:

- Ensures staff understand both generic cyber hygiene and their **specific control responsibilities**
- Reduces onboarding time for safe system access
- Supports compliance with AMC2 IS.I.OR.200(b)(5): “Security competence according to responsibilities”

2. Annual Refresher Training

Definition:

All personnel must complete an **annual ISMS refresher** covering evolving threats, updated internal policies, and real-life lessons learned. This training must be mandatory, traceable, and role-relevant.

Key Components:

a) Secure Handling of Digital Tech Logs

Context:
Digital aircraft tech logs (e.g. ETL/EFB systems) hold real-time defect data and maintenance history and are legally sensitive.

Training Elements:

- Logging into ETL systems using **MFA**
- Locking terminals after use and avoiding shared sessions
- Recognizing data integrity flags and reporting anomalies

Example:
An engineer leaving a tablet logged into the ETL system unattended on the flight deck—training ensures this is recognized as a **security breach** with operational consequences.

b) Safe Usage of Mobile Platforms

Context:
Tablets, smartphones, and laptops are commonly used for viewing task cards, recording work, or accessing work packs remotely. However, these are **high-risk endpoints**.

Training Elements:

- Avoiding unsecured Wi-Fi (e.g. at hotels or airports)
- Mandatory use of **VPN and corporate-approved apps only**
- Data encryption, lock-screen policies, and reporting lost/stolen devices immediately

Example:
A technician uses a personal phone to photograph a CRS on a whiteboard and shares it in an open messaging app—this violates both ISMS and airworthiness documentation rules.

c) Threat Recognition (Phishing, Social Engineering)

Context:
Frontline maintenance staff and support teams are increasingly targeted by attackers due to their access to aircraft configurations, maintenance status, and operational data.

Training Elements:

- Identifying phishing emails disguised as “M&E updates” or “MRO software patches”
- Recognizing voice-based social engineering (e.g., fake IT support)
- How to report suspicious activity immediately via ISMS hotline or ticketing platform

Example:
A planner receives an email requesting an urgent upload of an unverified AD compliance document—training helps them **recognize and escalate** rather than comply.

Training Validation & Records

- Training completion records are tracked in the HR/QA training management system.
- Post-training **knowledge checks** or scenario-based quizzes validate comprehension.
- **Non-compliance triggers access suspension** until remedial training is completed.

Conclusion: Embedding ISMS Culture in Maintenance Operations
A strong Training & Awareness framework:

- Transforms staff from passive users into **security-aware operational actors**
- Supports EASA compliance and strengthens audit readiness
- Builds a foundation for detecting, reporting, and preventing cyber-physical threats

All training programs should be updated **annually**, integrated into the Safety & Compliance Calendar, and supported by incident-driven feedback loops.

---

11. Continuous Improvement

- ISMS maturity reviewed quarterly
- Incidents drive updates to access control, training, and asset management
- Cross-department audit findings integrated into security roadmap

1. ISMS Maturity Reviewed Quarterly
Definition:
On a quarterly basis, the ISMS governance team—led by the Information Security Officer in coordination with Quality, Maintenance Planning, and IT—must review the system's maturity, using internal metrics, audits, incident reports, and improvement objectives.
Components of Maturity Review:

- Status of Key Performance Indicators (KPIs) such as:
  - Incident response time
  - Training completion rates
  - Control effectiveness audit scores
- Review of new regulatory requirements (e.g. updates to AMC/GM, Part-IS guidance)
- Progress against previous quarter's action items and milestones

Examples:

- Q1 Review identifies low compliance in USB control usage across outstations. Q2 action: enforce encrypted USB-only policy and reinforce training.
- Q2 Review includes outcomes of a phishing simulation; a 35% fail rate leads to Q3 remedial eLearning rollout.

Benefits:

- Keeps ISMS aligned with evolving risks and operational complexity
- Supports measurable, incremental progress
- Facilitates EASA oversight with documented evidence of governance and system performance

2. Incidents Drive Updates to Access Control, Training, and Asset Management

Definition:

Every significant security incident—whether cyber, procedural, or human-factor driven—should be investigated, root causes identified, and control changes implemented across relevant ISMS domains.

Mechanisms:

- Root Cause Analysis (RCA) linked to the Safety Management System (SMS)
- Corrective and Preventive Actions (CAPA) registered and tracked to closure
- Feedback loops to affected departments with cross-training or control reinforcement

Examples:

- **Access Control Update:**
  Following an incident where an engineer accessed CRS sign-off functions beyond their scope, RBAC policies were updated to include aircraft type-level restrictions.
- **Training Enhancement:**
  A malware infection caused by unverified email link access prompted an **additional phishing awareness module** to be added to annual training.
- **Asset Inventory Adjustment:**
  An incident involving a stolen tablet revealed it was not registered in the M&E asset management database. A new procedure was introduced requiring monthly reconciliation of all mobile assets.

Benefits:

- Ensures the ISMS is dynamic and evidence-driven
- Aligns technical and procedural safeguards to real operational gaps
- Reduces the likelihood of repeat failures and non-conformities

3. Cross-Department Audit Findings Integrated into Security Roadmap

Definition:

ISMS improvement activities are guided not only by security-specific audits but also by findings from **QA audits, operational audits, and external compliance reviews**, ensuring a holistic and unified approach to risk mitigation.

Integration Practices:

- QA and Security jointly review all findings from Part-145 internal audits with ISMS implications
- Non-conformities with security elements (e.g., expired access, incomplete records, insecure storage) trigger formal updates to the ISMS Security Roadmap
- Action items tracked in a centralised Risk and Compliance Dashboard

Examples:

- A routine QA audit finds that **task card PDFs** are stored on a shared folder without access controls—this is escalated to the ISMS team, which implements a SharePoint-based access-managed solution.
- An **EASA oversight visit** raises a finding regarding the lack of redundancy for the M&E server. The ISMS roadmap is updated with a Q4 objective to migrate critical services to a high-availability architecture.
- During a **SMS audit**, evidence of late reporting of system faults is noted. As a result, ISMS logs and anomaly detection alerts are integrated into weekly SMS reviews for better operational transparency.

Benefits:

- Creates a unified compliance and risk management strategy
- Drives investment prioritisation for security-related upgrades
- Enhances stakeholder accountability across CAMO, AMO, IT, and Quality

Conclusion: Making ISMS a Living System

Continuous improvement in a Part-145 ISMS must be:

- **Planned** – via structured governance reviews
- **Reactive** – to incidents and audit findings
- **Integrated** – with the wider safety and quality systems

Part 145 Risk Evaluation List to Review

Information Asset & Record Integrity Risks

1. Tampering with digital CRS (Certificate of Release to Service) records.
2. Unauthorised modification of component service history in M&E systems.
3. Loss or corruption of maintenance documentation during system outage.
4. Unsanctioned access to planning dashboards causing work schedule distortion.
5. Delayed data sync between CAMO and Part-145 resulting in inaccurate forecasts.

System Access and Identity Management Risks

6. Inactive user accounts exploited for credential-based attacks.
7. Shared logins on line station workstations undermining traceability.
8. Role creep: escalation of privileges without governance.
9. Lack of timely access revocation for departing subcontractors.
10. MFA bypass or failure leading to unauthorised remote access.

Tooling, Calibration & Job Card Risks

11. Corruption of calibration database resulting in use of unverified tools.
12. Tampered job card instructions causing procedural deviations.
13. Unauthorized print or duplication of sensitive job packs.
14. Use of outdated or unversioned task cards at line stations.
15. Poor access control for portable calibration devices and tooling kiosks.

Endpoint & Device-Related Risks

16. Malware introduced via USB devices during hangar activities.
17. Use of unprotected mobile devices to transmit maintenance data.
18. Loss or theft of tablets/laptops used for remote maintenance.
19. Insecure personal device connected to corporate Wi-Fi.
20. Discontinued OS or app versions used in field operations.

Maintenance-Critical Availability Risks

21. Outage of CRS portal halting aircraft dispatch operations.
22. Downtime in M&E systems (e.g., AMOS, TRAX) delaying heavy checks.
23. Inaccessibility of component traceability tools during inspections.
24. Failure of calibration database during audit or tool issuance.
25. Backup failure resulting in loss of signed job cards or digital tech logs.

Subcontractor & Third-Party Exposure Risks

26. VPN access granted to subcontractors using unsecured personal devices.
27. Submission of unauthenticated CRS documents from third parties.
28. Inadequate cyber hygiene of external AMOs causing interface vulnerabilities.
29. Misrouted task cards to subcontractors due to incorrect email sharing.
30. Non-compliant audit response practices from subcontracted providers.

OPS/CAMO Interface Vulnerabilities

31. MEL/CDL status data manipulated during live synchronization.
32. Deferred defect closures inaccurately reported or spoofed.
33. Aircraft readiness dashboard showing outdated or incorrect status.
34. Unauthorized OPS access to editable technical records.
35. Integrity failure in API delivering planning forecasts to maintenance.

Data Transmission and Storage Risks

36. Interception of task cards or CRS via unsecured email.
37. Use of public cloud storage for maintenance data without encryption.
38. Incomplete or unauditable record of data exchanged with CAMO.
39. Data mismatch between Part-145 and CAMO systems due to sync error.
40. Overexposed shared drives hosting unprotected safety-critical files.

Physical Security and Environmental Risks

41. Badge cloning or unauthorized access to tool cribs or server rooms.
42. Tampering with DVR/CCTV logs to cover up unauthorized entry.
43. Fire or flooding in calibration labs without offsite data redundancy.
44. Manipulation of physical task cards during inter-site transit.
45. Theft or loss of printed job cards/CRS from unsecured workbenches.

Training & Human Factor Risks

46. Engineers unaware of phishing/social engineering tactics.

47. Negligent handling of sensitive data on personal messaging apps.

48. Insufficient awareness of digital tech log protection protocols.

49. Non-compliance with secure USB use and encrypted data policies.

50. Staff bypassing secure portals for task access due to usability constraints.