

EASA Part 145 Cybersecurity Compliance Checklist

(Implementing Regulation (EU) 2023/203 without Additional Hiring)

This checklist helps EASA Part 145 organizations integrate cybersecurity into existing **SMS, Quality, and Compliance** functions, reducing reliance on external consultants.

1. Establish Internal Cybersecurity Governance

Assign Responsibilities

- Designate an **Information Security Focal Point (ISFP)** (can be an existing **Quality Manager, Safety Officer, or IT lead**).
- Integrate cybersecurity into **Quality & Safety Management System (SMS)**.
- Define cybersecurity roles in job descriptions of existing staff.

Develop Cybersecurity Policies & Procedures

- Establish an **Information Security Management System (ISMS)** aligned with **EASA Part 145 & ISO 27001**.
- Create **clear cybersecurity policies** for:
 - Access Control
 - Incident Response
 - Data Protection & Privacy
 - Supplier Cybersecurity Vetting
 - Employee Cyber Awareness
- Define **reporting structures for cybersecurity incidents**.

Limit External Access & Third-Party Risks

- Implement **Zero Trust Architecture** (No external party gets unrestricted access).
 - Require **Multi-Factor Authentication (MFA)** for IT administrators & remote workers.
 - Conduct **third-party cybersecurity risk assessments** for suppliers and IT contractors.
-

2. Implement Cybersecurity Controls (Using Existing IT Resources)

Protect IT & Maintenance Systems

- Secure **Maintenance Information Systems (MIS) & Part 145 record-keeping systems**.
- Apply **end-to-end encryption** for sensitive data (storage & transmission).
- Use **network segmentation** (separate critical maintenance networks from corporate IT).
- Conduct **regular software patching & vulnerability scanning**.

Restrict Unauthorized Access

- Implement **Role-Based Access Control (RBAC)** (limit access to "need-to-know" basis).
- Use **automated intrusion detection tools (IDS/IPS)** to monitor systems.
- Establish **privileged access management (PAM)** (control admin accounts).

Strengthen Cybersecurity Awareness

- Provide **basic cybersecurity training** for all employees.
 - Conduct **monthly phishing simulation exercises** to prevent social engineering attacks.
 - Assign **cyber hygiene responsibilities** (password management, secure file handling).
-

3. Conduct Cyber Risk Assessments & Audits

Regular Cybersecurity Risk Assessment

- Map all **critical IT systems & data flows** (maintenance records, software, supplier access).
- Identify **potential vulnerabilities** (legacy systems, third-party software).
- Classify risks using **EASA-approved risk assessment methodology**.
- Mitigate unacceptable risks using:
 - Firewalls & Intrusion Detection
 - Regular **penetration testing** (can be automated, no need for external consultants)
 - Backups & Disaster Recovery Plans**

Internal Cyber Audits (Integrated with Quality Audits)

- Conduct **cybersecurity self-audits** every 6 months.
- Align audits with **EASA Part 145 & ISO 27001 standards**.

- Ensure **supplier compliance** with cybersecurity policies.
-

4. Establish Incident Detection, Response & Reporting

Develop Cybersecurity Incident Response Plan

- Create a **step-by-step Cyber Incident Response Plan (IRP)** based on EASA IS.I.OR.220.
- Define **incident categories** (e.g., phishing, ransomware, unauthorized access).
- Establish **internal escalation process** (who gets notified & when).

Incident Detection & Response

- Enable **real-time monitoring** of IT networks (using automated detection tools).
- Conduct **"tabletop" cyberattack drills** every 6 months (simulated response scenarios).
- Establish a **forensic investigation procedure** (to analyze root causes & prevent recurrence).

Regulatory Reporting (Internal & External)



- Report **high-risk incidents** to the **National Aviation Authority (NAA)** within **72 hours**.
- Use **EASA-approved cybersecurity reporting format** (aligned with ECCAIRS).
- Maintain **detailed incident logs for 5 years** (per IS.I.OR.245).

5. Continuous Improvement & Compliance Monitoring

Cybersecurity Performance Monitoring

- Track cyber incidents & trends (to identify weaknesses).
- Benchmark cybersecurity maturity using ISO 27001 risk assessment models.
- Periodically update cybersecurity policies based on new threats.
- Integrate Cybersecurity into SMS & Change Management**
 - Ensure cybersecurity is part of safety risk assessments & safety committees.
 - Apply cyber risk evaluation to any system changes (e.g., new software, cloud migration).
 - Regularly review and update ISMS in compliance with EASA Part 145 & Regulation (EU) 2023/203.

Implementation Timeline (*Without Hiring Extra Staff*)

-  **Phase 1: Setup (0-2 months)**
 - Assign cybersecurity focal point & responsibilities
 - Establish cybersecurity policies & ISMS
 - Secure supplier access & limit third-party risks
-  **Phase 2: Cyber Risk Assessments & Controls (2-6 months)**
 - Conduct cybersecurity risk assessment

✓ Implement security controls (firewalls, encryption, MFA)

✓ Train employees on cybersecurity awareness

July
17

Phase 3: Incident Response & Reporting (6-9 months)

✓ Develop & test Cyber Incident Response Plan (IRP)

✓ Set up internal & external reporting structures

July
17

Phase 4: Audits & Continuous Monitoring (9-12 months & ongoing)

✓ Conduct first internal cyber audit

✓ Start continuous monitoring & update policies

Conclusion

By following this checklist, EASA Part 145 organizations can achieve **full cybersecurity compliance without hiring new staff** by:

✓ **Training existing personnel** instead of hiring external consultants

✓ **Integrating cybersecurity into existing SMS & Quality functions**

✓ **Using automated cybersecurity tools** to minimize workload

✓ **Limiting third-party access & controlling supply chain risks**

This reduces dependency on external cybersecurity firms, keeping your organization's **data, maintenance records, and IT infrastructure secure** while staying compliant with **Regulation (EU) 2023/203**.