Meeting the Challenge of complying with EASA Information & Cyber Security obligations without the need to recruit Additional Manpower

Sofema Online (SOL) Takes a deep dive into meeting the Information Security & implementation challenges without recruiting additional manpower.

Introduction - IT and cybersecurity are so specific that companies often have to hire new people or even hire outside people to set up, manage and test/audit. Concerns regarding the reliance on external cybersecurity consultants and contractors in EASA Part 145 organizations are valid and shared among many stakeholders in the industry.

The **SAS Part 145 Cyber Security Implementation course** you provided covers **third-party cybersecurity risks** extensively and highlights supply chain security as a critical concern for compliance with **Regulation (EU) 2023/203**.

Instead of hiring additional personnel or outsourcing, **EASA Part 145 organizations can**:

✔ **Train existing staff in cybersecurity awareness and ISMS implementation**
✔ **Embed cybersecurity into SMS, quality, and compliance roles**
✔ **Use automated tools for monitoring, detection, and reporting**
✔ **Control third-party access and strengthen supply chain security**

This approach ensures compliance **without increasing overhead costs or exposing critical IT systems to external risks**.

Key Points on Managing Cybersecurity Without Hiring Additional Manpower

1. **Leverage Existing Personnel with Targeted Training**
    - EASA **does not mandate hiring dedicated cybersecurity personnel**. Instead, it requires integrating cybersecurity into existing Safety Management Systems (SMS).
    - Internal staff can be trained to manage **Information Security Management Systems (ISMS)**, risk assessment, and compliance.
    - Training programs, such as those offered by **Sofema Online**, can upskill **quality managers, safety officers, and IT personnel** to handle cybersecurity without expanding headcount.
2. **Integrate Cybersecurity into Existing SMS & Compliance Roles**
    - Cybersecurity can be embedded into **existing quality assurance, compliance, and safety management teams** to ensure efficiency without duplication of roles.

- The **Accountable Manager, Nominated Post Holder, and Compliance/Safety Manager** already have **defined cybersecurity duties** under the regulation, removing the need for additional specialists.

3. **Implement Risk-Based Approach with Automated Monitoring**
    - Instead of hiring dedicated cybersecurity staff, organizations can use **intrusion detection systems (IDS), automated vulnerability scanning, and endpoint security tools** to monitor threats.
    - These tools **reduce dependency on external consultants** by enabling **real-time monitoring** and **early detection** of cyber threats.
4. **Control Third-Party & Supplier Cybersecurity Risks**
    - **External consultants and suppliers** pose a risk if they have unrestricted access to **critical IT systems, aircraft maintenance records, or operational data**.
    - EASA Part 145 organizations should implement **strict access control measures**, such as:
        - **Zero Trust Architecture** (assume breach, restrict access by role).
        - **Multi-Factor Authentication (MFA)** for remote and privileged access.
        - **Supplier Cybersecurity Vetting** (third-party risk assessments and contractual obligations for cybersecurity compliance).
5. **Strengthen Incident Response Without External Dependence**
    - A **clear internal response plan**, including **staff awareness training and simulation exercises**, ensures rapid action without relying on expensive external auditors.
    - **Internal reporting systems** (aligned with **ECCAIRS methodology**) allow **employees to escalate cybersecurity issues** within the organization rather than exposing them to outsiders.

Shared Concerns Among Industry Stakeholders

- **Supply Chain Security Risks**
    - The **NIS2 Directive (EU) 2022/2555** highlights the vulnerabilities introduced by third-party providers, requiring organizations to **evaluate and control vendor access to critical systems**.
    - The SAS course material specifically warns about **third-party cybersecurity risks** in maintenance environments.

- **Threats from External IT Consultants**
    - External cybersecurity consultants **often have privileged access**, making them a potential attack vector.
    - Best practice is to **limit consultant access strictly** and ensure that **internal personnel oversee all cybersecurity implementations**.
- **Regulatory Compliance Without New Hiring**
    - **EASA acknowledges that many Part 145 organizations lack in-house cybersecurity expertise** but does not mandate recruitment.
    - Instead, compliance can be achieved through **training existing staff, adopting automated tools, and integrating cybersecurity into SMS/quality assurance functions**.

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

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

✅ Develop & test Cyber Incident Response Plan (IRP)
✅ Set up internal & external reporting structures

📅 **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**.