# Cybersecurity Checklist for EASA Part 145 Organizations - Sofema Aviation Services_Jan_25_R1

## Threat Identification and Assessment

☐ Document external threats (e.g., malware, phishing, DDoS, cyber-espionage).
☐ Assess internal threats, including human error and insider risks.
☐ Evaluate systemic vulnerabilities (legacy IT systems, third-party software weaknesses, weak authentication mechanisms).
☐ Assess supply chain cybersecurity risks, including third-party vendor weaknesses.
☐ Identify emerging threats, including IoT device compromises and AI-driven attacks.
☐ Conduct regular risk assessments and document findings in a risk assessment report.

## Policy Development and Documentation

☐ Develop policies in compliance with Regulation (EU) 2023/203.
☐ Include detailed policies for risk management, incident response, and data protection in the ISMS.
☐ Create and maintain an Information Security Management Manual (ISMM) with cybersecurity protocols.
☐ Define a structured amendment process for the ISMM.

## Role Assignment and Training

☐ Assign roles and responsibilities (e.g., Accountable Manager, Compliance Manager, Safety Manager).
☐ Establish competency requirements for ISMS-related roles.
☐ Conduct cybersecurity training for all employees, contractors, and third-party vendors.
☐ Update training programs annually to address evolving threats and vulnerabilities.
☐ Promote a culture of cybersecurity awareness and proactive reporting.

## Implementation of Technical Controls

☐ Implement firewalls, intrusion detection systems, and secure communication protocols.
☐ Ensure encryption methods and multifactor authentication are in place.
☐ Vet vendors and third-party service providers for cybersecurity compliance.
☐ Test diagnostic systems, maintenance software, and IT infrastructure for vulnerabilities.
☐ Utilize automated tools to detect unusual activity and track vulnerabilities.

## Incident Response and Management

☐ Establish an incident response plan (IRP) with roles and responsibilities for containment, mitigation, and recovery.
☐ Simulate incident scenarios, such as phishing attacks and ransomware incidents, to test readiness.
☐ Ensure contact points for internal and external reporting are established (e.g., local authorities, EASA).
☐ Maintain records of all cybersecurity incidents and analyze them for lessons learned.

## Continuous Monitoring and Auditing

☐ Conduct regular internal audits to confirm compliance with Regulation (EU) 2023/203.
☐ Use findings from audits and incident reviews to refine processes.
☐ Integrate cybersecurity into the organization's internal audit program.
☐ Report audit findings to the Accountable Manager.

## Annual Review and Continuous Improvement

☐ Conduct a comprehensive risk reassessment annually to identify new threats.
☐ Address emerging vulnerabilities and update security controls accordingly.
☐ Review and improve the incident response plan based on lessons learned.
☐ Re-evaluate vendors and third-party providers for ongoing compliance.
☐ Document and implement continuous improvement initiatives, such as adopting new technologies.

## Oversight of Contracted Activities

☐ Verify that contractors comply with ISMS requirements.
☐ Monitor and audit third-party activities regularly to ensure alignment with cybersecurity policies.

## Documentation and Record-Keeping

☐ Maintain detailed records of risk assessments, training, and incidents.
☐ Ensure documentation provides clear cross-references to ISMS requirements.

## Call to Action

Organizations should use this checklist to ensure comprehensive cybersecurity measures are implemented and maintained, safeguarding critical systems and complying with aviation safety standards. For tailored training and guidance, visit Sofema Aviation Services (www.sassofia.com) or Sofema Online (www.sofemaonline.com).