EASA Compliant Cyber Security Audit Checklist

1. EASA Compliant Cyber Security Audit Checklist:

- Ensure alignment of Cyber Security Policy with EASA guidelines
- Define and document roles and responsibilities for Cyber Security within the organization
- Identify and document the assets requiring protection and associated risks

2. Risk Assessment and Management

- Implement a process for risk assessment of critical systems, networks, and infrastructure
- Identify potential threats and vulnerabilities specific to aviation systems
- Establish processes for risk mitigation strategies and controls based on assessment results

3. Breach Reporting

- Develop procedures for reporting cyber incidents and data breaches to relevant authorities, including EASA
- Maintain detailed records of all incidents, response actions, and lessons learned
- Create a procedure for the management of data breach notification

4. Staying Updated with EASA Guidelines

- Regularly review and update the Cyber Security program to align with the latest EASA guidelines
- Engage continually with new threats, vulnerabilities, and best practices in the aviation industry

5. Cyber Security Management

- Establish a comprehensive cybersecurity management program
- Designate a person or team for cybersecurity oversight
- Document and communicate cybersecurity policies and procedures
- Clearly define and communicate cybersecurity roles and responsibilities
- Conduct a risk assessment to identify cybersecurity threats and vulnerabilities

- Deploy anti-malware solutions and regularly update software
- Educate employees on cybersecurity best practices

6. Cyber Security Incident Response

- Develop an incident response plan and review it periodically
- Implement mechanisms to monitor, detect, and respond to cybersecurity incidents
- Establish a system for reporting and documenting cybersecurity incidents

7. Cyber Security Software & Controls

- Implement access controls for sensitive systems and data
- Regularly update software applications and operating systems with security patches
- Deploy and update antivirus and anti-malware solutions
- Implement network security measures like firewalls and intrusion detection systems
- Conduct regular employee training on cybersecurity best practices
- Assess and impose cybersecurity obligations on third-party vendors and partners

8. Cyber Emergency Response System

- Document a Cyber emergency response plan
- Designate an emergency response team for coordination and execution
- Communicate the Cyber emergency response plan to stakeholders and personnel
- Conduct Cyber emergency response drills and exercises
- Establish a system for emergency alerts and notifications
- Maintain established communication channels and protocols during emergencies
- Ensure backup systems and redundancies for continuous operations
- Identify critical assets and systems for special protection during emergencies
- Develop contingency plans to mitigate potential risks and disruptions
- Establish coordination with relevant authorities and agencies for emergencies
- Implement procedures to assess and manage risks associated with emergency response
- Review and update the emergency response plan based on lessons learned