EASA Part 145 Hardware Audit and Assessment - Hardware Inventory and Scope

Regulatory Drivers IS.I.OR.205(a)(2)/IS.D.OR.205(a)(2)

- Is there a current and comprehensive inventory of all hardware assets (equipment, systems) that contribute to the functioning of safety-related activities/services?
- Is the hardware explicitly covered within the defined scope of the ISMS? (GM1 IS.I.OR.205(a)/GM1 IS.D.OR.205(a))
- IS.I.OR.205(b)/IS.D.OR.205(b) Are interfaces that the hardware has with other organisations (e.g., supply chain, service providers) documented to identify mutual exposure to information security risks? (AMC1/GM1 IS.I.OR.205(b)/IS.D.OR.205(b))

Risk Assessment & Review IS.I.OR.205(c)/IS.D.OR.205(c)

- Are information security risks specific to the hardware (e.g., physical tampering, data loss on device) that could impact aviation safety identified?
- Is a risk level assigned to each hardware-related risk using a predefined classification that considers potential of occurrence (e.g., exploitation of hardware vulnerability) and severity of safety consequences?

IS.I.OR.205(d)/IS.D.OR.205(d)

- Is the hardware risk assessment regularly reviewed and updated upon changes to the hardware/system, interfaces, or lessons learned from incidents? (AMC1 IS.I.OR.205(d)/IS.D.OR.205(d))

Risk Treatment (Controls) IS.I.OR.210(a)/IS.D.OR.210(a)

- Are measures (controls) developed and implemented to address unacceptable risks associated with the hardware? (e.g., physical access controls, hardening/security configuration, secure disposal)
- Is there evidence of checking the continued effectiveness of hardware security controls (e.g., regular physical audits, penetration tests against connected systems)?

IS.I.OR.210(b)/IS.D.OR.210(b)

- Is the relevant personnel informed of the risks shared at interfaces concerning hardware (e.g., hardware procured from a specific supply chain)?

Incident Management IS.I.OR.220(a)/IS.D.OR.220(a) (b) (c)

- Are measures implemented to detect events/vulnerabilities that could indicate potential materialization of unacceptable risks on the hardware? (e.g., physical security alarms, network monitoring for hardware, regular scanning for vulnerabilities in hardware-specific software/firmware)
- Are there predefined response measures to contain the spread of an attack involving compromised hardware and to control its failure mode?
- Are there recovery measures and a defined recovery time to restore the affected hardware elements to a safe state? (AMC1 IS.I.OR.220(c)/IS.D.OR.220(c))

Contracting of Activities IS.I.OR.235(a)/IS.D.OR.235(a)(b)

- If hardware-related management activities (e.g., maintenance, security monitoring) are contracted out, is the contracted organisation subject to oversight and are the associated risks appropriately managed?
- Does the contract ensure the competent authority has access upon request to the contracted organisation to verify continued compliance related to the hardware provision/service? (AMC1 IS.I.OR.235(b)/IS.D.OR.235(b))

Record-Keeping IS.I.OR.245(a)(1)(iv)/IS.D.OR.245(a)(1)(iv) (d)

- Are records of risks identified in the hardware-related risk assessment, along with associated risk treatment measures, archived and traceable?
- Are records (e.g., audit logs from hardware systems, configuration baselines) protected from damage, alteration, and theft, ensuring their integrity, authenticity, and authorised access?

Personnel IS.I.OR.240(i)/IS.D.OR.240(i)(g)

- Is the identity and trustworthiness of personnel who have access to the information systems and data (including hardware) appropriately established?
- Is there a process to ensure that personnel responsible for the hardware (e.g., maintenance, administration) have the necessary competence (knowledge, skills, and experience)?

Risk Treatment Notes - Based on the EASA Part 145 Hardware Audit and Assessment document, the task descriptor for mitigation in relation to the risk assessment category (Lo – Med- Hi) must align with the Risk Treatment (Controls) and Incident Management requirements of the EASA Information Security Management System (ISMS) regulations (IS.I.OR.210(a)/IS.D.OR.210(a) and IS.I.OR.220/IS.D.OR.220).

The overall task is to ensure that unacceptable risks identified during the hardware-related risk assessment are addressed by appropriate security controls and incident response measures.

Task Descriptor: Hardware Risk Mitigation and Control Implementation

1. Risk Treatment (Controls)

Develop, implement, and maintain security measures (controls) to address unacceptable risks associated with hardware assets that could impact aviation safety, as defined by the Risk Assessed Category.

- **Actionable Steps and Requirements:**
    - For hardware risks classified as Medium (Med) or High (Hi), develop specific measures/controls (e.g., physical access controls, hardening/security configuration, secure disposal protocols).
    - Implement the agreed-upon controls, ensuring they are documented and aligned with the assigned risk level.
    - Establish a process for regularly checking the continued effectiveness of implemented hardware security controls (e.g., periodic physical audits, penetration tests against connected systems).
    - Ensure relevant personnel are informed of shared risks at interfaces concerning the hardware (e.g., supply chain hardware).
    - Archive and ensure traceability of records detailing risks identified, the assigned risk level, and the associated risk treatment measures (controls).

2. Incident Management and Resilience

Implement and maintain measures to detect, respond to, and recover from events, vulnerabilities, or incidents that could materialize unacceptable risks on the hardware.

- **Actionable Steps and Requirements:**
    - Implement **detection measures** for events/vulnerabilities that could indicate potential materialization of unacceptable hardware risks (e.g., physical security alarms, network monitoring, regular scanning for vulnerabilities in hardware-specific software/firmware).

- Establish and document **predefined response measures** to contain the spread of an attack involving compromised hardware and to control its failure mode.
- Define and implement **recovery measures** and a **defined recovery time** (RTO - Recovery Time Objective) to restore affected hardware elements to a safe state following an incident.

3. Oversight for Contracted Activities (If Applicable)

If hardware-related management or security activities (e.g., maintenance, security monitoring) are contracted out, ensure appropriate oversight and risk management.

- **Actionable Steps and Requirements:**
  - Verify the contracted organisation is subject to oversight and that the associated hardware risks are managed appropriately.
  - Ensure contracts guarantee the competent authority access to the contracted organisation to verify continued compliance related to the hardware service.

Business Area	Equipment Description Part No Serial Number	Risk Assessed Category Lo – Med-Hi	Comments – Additional Actions Required

