EASA Part 145 and ISO/IEC 27001 Risk Register Considerations

The following risks address critical areas of information security (IS) and align with the requirement to establish, implement, maintain, and continually improve an Information Security Management System (ISMS), as detailed in EASA Part IS and principles of ISO/IEC 27001.

1. Access Control and Identity Management (A.9 in ISO 27001)

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
1	Credential theft through phishing, spoofed portals, or social engineering	Non-implementation of strong **authentication controls** and **security awareness training**.
2	Weak or reused passwords across critical systems without MFA enforcement	Failure to enforce a **strong authentication policy** (e.g., mandatory MFA).
3	Failure to revoke digital access after staff departure or contractor offboarding	Deficiency in the **user access provisioning and de-provisioning process**.
4	Shared or orphaned third party accounts with persistent privileges	Failure in **account management**; non-adherence to the **principle of least privilege**.
5	Insider threats due to over-permissioned user roles	Poor definition and implementation of **role-based access control (RBAC)**.
18	Delayed revocation of physical access (badges, keys)	Deficiency in the **physical and environmental security policy** and its execution.
19	Badge cloning or tailgating leading to unauthorized access	Failure in **physical access monitoring and control**.

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
57	Biometric access systems overridden or spoofed	Failure of **physical access control mechanisms** and their associated security design.

2. Operational Security and Asset Management (A.8, A.12 in ISO 27001)

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
10	Unmonitored use of portable maintenance devices without endpoint controls	Lack of **endpoint detection and response (EDR)** or other **mobile device management (MDM)** controls.
11	Malware introduction via USBs or infected subcontractor devices	Failure of **malware protection** and **removable media controls**.
12	Data loss during offline tablet usage or delayed sync	Risk to **data integrity and availability** due to unmanaged data states.
14	Unauthorized MEL/CDL edits or deferred defect tampering	Critical failure in **change control** and **system integrity** for airworthiness data.
15	Lack of centralized logging and audit trails for critical systems	Non-compliance with **monitoring and logging** requirements; inability to perform incident investigation.
21	Unattended consoles in dispatch or maintenance environments	Failure to enforce a **clear screen and clear desk policy**.
26	Lack of asset classification or criticality prioritization	Deficiency in the **asset management** and **information classification** process.
47	Exposure of unprotected critical files on shared drives	Poor implementation of **storage access control** and **data leakage prevention**.

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
51	Incomplete IT asset inventory or software list	Deficiency in **asset inventory management**, undermining the ISMS scope and control baseline.
52	Poor internal network segmentation across business units	Failure in **network security architecture** to isolate critical systems.
53	Simultaneous backup and production outage from shared access	High **availability risk** due to poor segregation of duties and access.

3. System Development and Maintenance (A.14 in ISO 27001)

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
9	Legacy systems with unsupported OS or weak encryption	Failure to manage **vulnerabilities** and maintain current software; use of insecure technologies.
14	Unauthorized MEL/CDL edits or deferred defect tampering	Integrity failure in **airworthiness data systems** requiring secure configurations.
25	Absence of audit trail on CRS, MEL, or AMP updates	Non-compliance with **audit logging for critical configuration changes**.
30	Hardcoded API tokens or exposed integration keys	Failure in **secure coding practices** and **management of secret keys**.
32	CRM or loyalty platform exploited via API vulnerabilities	Lack of **security testing** and **vulnerability management** for APIs.
55	Lack of centralized control over aircraft software versions	Critical failure in **configuration management** for airworthiness-impacting systems.

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
56	Use of discontinued or unsupported mobile apps in operations	Failure in **software lifecycle management** and associated security reviews.

4. Communication Security and Data Protection (A.13, A.18 in ISO 27001)

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
6	Use of unsecured Wi-Fi by staff using tablets or mobile devices	Failure to enforce a **secure mobile working policy** and **network security standards**.
10	Unencrypted or insecure data exchange with third parties	Non-compliance with **data in transit security** requirements; lack of **secure transfer protocols**.
14	Cross-contamination between secure and non-secure devices or systems	Failure to enforce **segregation** between business-critical and personal/unsecured environments.
23	Data leakage from unencrypted email (e.g. AMP, job cards)	Lack of **encryption controls** for sensitive information (like AMP/job cards) in email.
24	Use of personal apps or unauthorized file-sharing platforms	Deficiency in **acceptable use policy** and **data exfiltration controls**.

5. Third-Party and Vendor Management (A.15 in ISO 27001)

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
16	Insecure cloud hosting without formal DPA/SLA	Failure to establish **Information Security requirements in supplier agreements** (DPA/SLA).
17	Lack of vendor ISMS governance or third-party security clauses	Deficiency in **supplier security due diligence** and **contractual IS requirements**.
45	Unsecured third-party VPN or endpoint access	Risk introduced by **supplier remote access**; failure to enforce organization security standards.
46	Subcontractor access without cyber hygiene enforcement	Lack of **monitoring** and **security enforcement** for external users.

6. Incident Management and Business Continuity (A.17 in ISO 27001)

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
13	Backup failures or lack of tested disaster recovery plans	Non-compliance with **availability requirements**; absence of a proven **Disaster Recovery Plan (DRP)**.
29	Denial of Service (DoS) targeting slot coordination or CTOT tools	Risk to **operational availability**; failure to implement **resilience measures**.
35	Loss or corruption of technical records (electronic or physical)	Failure in **records management** and **data integrity/availability**.
33	SIEM blind spots or failed detection of anomalies	Inadequate **security monitoring** capability, leading to delayed **incident detection**.

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
35	No defined ISMS incident response playbooks or protocols	Failure to establish a formal **Information Security Incident Management (ISIM) process**.
36	No cross-role BCP training or simulation drills	Lack of **Business Continuity Plan (BCP) testing and readiness**.
38	Role confusion during cyber incident response	Deficiency in the **ISIM process**; lack of defined roles and responsibilities.
46	Emergency plan failure due to poor interdepartmental execution	Lack of **integrated BCP/DRP testing** across operational units.

7. Human Resources and Compliance (A.7, A.18 in ISO 27001)

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
34	Shadow IT usage by management or departments during crises	Failure to enforce **acceptable use** and **non-standard IT policy**.
37	Lack of awareness in phishing, malware, or cyber hygiene	Failure in the **Information Security Awareness, Education, and Training** program.
39	Improper disposal of physical records (e.g., customs, rosters)	Failure to adhere to **secure disposal and de-commissioning policies**.
40	Use of outdated or manipulated calibration records or task cards	Risk to **data integrity** and **airworthiness** due to uncontrolled data.

Risk ID	Original Risk Item	Compliance Focus (EASA Part IS / ISO 27001)
41	Integrity failures in tooling and component traceability systems	Failure to ensure the **security of physical and digital assets** necessary for maintenance.
44	Non-compliance with AMC1 IS.I.OR.200(e) requirements	Direct **regulatory compliance failure** with EASA Part IS.
48	Outdated ISMS policies or delayed regulatory updates	Failure in the **ISMS maintenance** and **continual improvement** process.
49	Failure to implement ISMS audit findings or corrections	Deficiency in **corrective action** and **non-conformity management** following internal or external audits.
54	Third-party CRS submission lacking digital verification	Failure to enforce **non-repudiation** and **digital signature/verification** for critical documents.