SOFEMA
AVIATION SERVICES

**Information Security Risk Register: Potential Issues - Integrated Operator**

**1. Unauthorized Access to Operational Systems**

Inadequate access controls leading to exposure of Departure Control System (DCS), Load Control, or Baggage Reconciliation System BRS platforms to unauthorized or under-trained staff.

2. **Credential Compromise via Phishing or Spoofing**

Spoofed login portals or social engineering enabling credential harvesting, particularly in check-in and dispatch environments.

3. **Unsecured Mobile Devices on Untrusted Networks**

Tablets used for remote boarding or ramp operations connecting via open Wi-Fi, enabling MitM attacks. - A Man-in-the-Middle (MitM) attack is a cyberattack where a malicious actor secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other.

4. **Data Integrity Failures in Load Control Systems**

Altered weight and balance data due to software bugs, insider manipulation, or malware intrusion.

5. **Inadequate MFA Enforcement Across Platforms**

Absence or inconsistent application of Multi-Factor Authentication (MFA) on terminals, handhelds, or admin portals.

6. **System Downtime Impacting Critical Functions**

Outages in Cargo Management System - CMS, BRS, or W&B tools leading to ground delays, mishandling, or compromised safety margins.

7. **Failure to Revoke Access Post-Contract Termination**

Dormant user accounts left active after staff departure or contractor disengagement, posing privilege escalation risks.

8. **Human Error in Data Entry or Manual Overrides**

Ramp or check-in staff inputting incorrect data (e.g. ULD weights, baggage tags), bypassing system checks.

9. **Legacy Systems with Weak or No Encryption**

Baggage systems, kiosks, or dispatch software using outdated protocols for data transmission.

10. **Insecure Data Exchange with Third Parties**

Contractors (e.g. catering, ground handling) transmitting provisioning or manifest data over unencrypted channels.

11. **Insider Threat from Over-Permissioned Staff**

Access privileges not aligned with operational need (e.g. admin-level access to junior baggage staff).

12. **Loss or Theft of Physical Devices**

Handheld scanners or tablets misplaced during shift change, storing unencrypted PNR or baggage data.

13. **Supply Chain Risk from Non-Compliant Vendors**

Third-party systems (CMS, catering) introducing vulnerabilities due to poor patching or non-certification.

14. **Spoofed or Manipulated Service Requests**

Unauthenticated commands issued to fueling, pushback, or cleaning dispatch systems.

15. **Malware Introduction via USB or Shared Workstations**

Removable media used by external vendors infecting central operational systems.

16. **Unsegmented Networks Between Departments**

Shared infrastructure between AMO, CAMO, Ops, and Security exposing cross-domain vulnerabilities.

17. **Inaccurate or Conflicting Load Sheet Versions**

Lack of version control leading to misaligned data across OFP, dispatch, and load control systems.

18. **Compromised CCTV and Monitoring Terminals**

Unauthorized access to or recording of CCTV feeds showing operational movements or personnel.

19. **Improper Disposal of Confidential Physical Records**

Load sheets, rosters, or customs documents discarded without shredding or locked storage.

**20. Delayed Revocation of Physical Access Credentials**

ID badges or vehicle keys active after shift changes or access right updates not synchronized.

21. **Compromised Customs Interface or DG Documentation**

Intercepted or altered cargo declarations between CMS and customs portals.

**22. Cross-Contamination Between Secure & Non-Secure Devices**

Shared devices between secure (e.g., customs, load planning) and non-secure (e.g., service logs) applications.

**23. Failure to Classify and Prioritize Critical Assets**

Lack of clear identification of mission-critical assets such as W&B tools, DCS, or OFP platforms.

**24. Inadequate Incident Detection and Response Maturity**

No active monitoring or playbooks for ransomware, credential misuse, or system denial events.

**25. Non-Conformance with IS.I.OR Requirements (203/2023)**

Missing controls for incident classification, asset documentation, or stakeholder mapping per regulation.

**26. Data Loss from Improper Offline Synchronization**

Scanner or tablet events not uploading post-network outage, leading to reconciliation errors.

**27. Lack of Formal Vendor Security Governance**

Absence of SLAs, audits, or compliance clauses for third-party contractors with system access.

**28. Training Gaps in Role-Specific ISMS Procedures**

Staff unaware of phishing, device usage, or response protocols due to infrequent or untargeted training.

**29. Insecure Hard Copy Documentation Practices**

Open access to printouts of sensitive reports, shift rosters, or incident logs.

**30. Failure to Maintain ISMS Documentation & Evidence**

Incomplete ISMS logs, incident records, or audit evidence undermining compliance and response capability.

**31. Weak User Passwords in CAMO Planning System**

**32. Insecure Email Transfer of Work Packages**

Use of email for PDF sharing

**33. Unauthorized AMO Access to AMP Tables**

Misconfigured access roles

**34. Legacy EFB App with Known Vulnerabilities**

Unpatched mobile app

**35. Incomplete Backup of Technical Records**

Manual backup routine

**36. Generic Login Accounts Shared Among Staff**

Lack of individual accountability

**37. Phishing Risk to CAMO Admin Staff**

Social engineering

**38. Contractors Retaining System Access Post-Project**

Failure to deactivate accounts

**39. Insecure Wi-Fi Used by Line Maintenance Staff**

Personal or public networks

**40. Missing Security Patches on CAMO Workstations**

Irregular patching schedule

**41. No Audit Trail on MEL Status Updates**

System lacks logging

**42. Data Leakage from Uncontrolled USB Ports**

No USB restriction policy

**43. Third-Party AMO Connects via Untrusted Network**

Insecure remote access

**44. No Centralised Logging for CAMO–OCC Data Exchange**

Fragmented tools

**45. Lack of Data Classification Policy**

Absence of asset tagging

**46. Technical Records Stored on Non-Encrypted Drives**

Insecure storage

**47. Uncontrolled Use of File-Sharing Apps (e.g., WeTransfer)**

Shadow IT

**48. No Business Continuity Plan for CAMO IT Systems**

BCP not established

**49. Excessive Access Privileges for Temporary Staff**

Temporary or contract CAMO personnel assigned permanent system

**50. Unmonitored Use of Portable Maintenance Devices**

Tablets/laptops used for remote aircraft defect entry not centrally monitored

**51. Technical Log Copies Circulated as Unprotected PDFs**

Exported PDFs shared across departments without encryption

**52. Lack of Alerting on Critical System Changes**

No notification when AMP tasks, MEL entries, or deferred defects are changed

**53. Third-Party Cloud Hosting Without Formal DPA or SLA**

Use of cloud-based CAMO planning module with no signed Data Processing Agreement (DPA) or Service Level Agreement (SLA)

**54. Absence of a Defined Incident Response Process**

CAMO staff unsure how to report or escalate cyber incidents

**55. Shared EFB Login Credentials for MEL Management**

Crew use common credentials to access MEL updates during flight

**56. CAMO Risk Register Not Integrated with SMS System**

Cyber risks and ISMS risks not reflected in enterprise-wide safety system

**57. Aircraft Software Revisions Not Version-Controlled**

CAMO lacks visibility of software configurations and patches installed by AMO

**58. CAMO Asset Inventory Incomplete or Outdated**

No validated record of laptops, mobile devices, software tools in CAMO use

**59. Hardware: Server downtime, loss of asset control, AOG data station vulnerabilities**

Malware infection, misconfigured work order systems, version mismatch, People: Social engineering, accidental data disclosure, competence gaps, Poor access control, shared network breaches, loss of audit trail

**60. Server Downtime During Peak Planning Periods**

maintenance scheduling system hosted on a local server becomes unavailable during a heavy aircraft maintenance period.

**61.Impact: Risk of data theft or loss following physical theft.**

**62. AOG Support Device Exposure at Remote Stations**

**63. Malware Infection via Infected Maintenance USBs**

AMO personnel introduce malware into CAMO systems by using removable drives during a maintenance event.

**64. Human factors—including intentional or unintentional behavior by employees, contractors, or third parties—pose significant exposure in CAMO operations.**

Social Engineering Attack on CAMO Planning Staff

**65. CAMO team members lack training in proper use of data classification, secure communication, or incident reporting.**

Misuse of systems, unreported breaches.

**66. Poor Access Control Policies Across Shared Systems**

AMO users retain access to CAMO planning modules after project completion.

**67. A malware infection in an AMO maintenance kiosk propagates to CAMO systems through an inadequately segmented network.**

Compromise of airworthiness management applications.

**68. Delayed Board-Level Threat Awareness**

Cyber incidents not escalated promptly, undermining strategic BCP decisions.

**69. Use of Shadow IT by Executives – Unauthorized apps/devices bypass enterprise controls during crises.**

**70. Fragmented Incident Playbooks – Inconsistent or outdated departmental BCP guidance results in uneven recovery**.

**71. Lack of Policy Harmonization Across Units – Incoherent application of ISMS–BCP directives increases regulatory exposure.**

**72. Third-Party Non-Conformance – Suppliers fail to meet ISMS-related BCP controls (e.g., CRM or EFB vendors).**

**73. Operational Continuity Risks (OCC, Dispatch, Flight Ops)**

**74. Maintenance & Airworthiness Systems**

Tampering with Deferred Defect Data – Alters MEL/CDL logs, compromising airworthiness.

**75. DDoS Against Booking/Check-in Portals – Impacts brand reputation and revenue during peaks.**

**76. CRM Exploitation – Loyalty or payment data stolen due to third-party API weakness.**

**77. Safety Reporting System Downtime –**

Obstructs timely SMS hazard communication and incident escalation.

**78. Central IT Compromise (APT/Firmware) – Impacts PSS, OCC, and Maintenance via domain controller or firmware attack.**

**79. Power Loss Without Proper Failover –**

Single-point outage disables primary systems without effective failover.

**80. Delayed Incident Escalation –**

Incorrect severity classification delays BCP activation.

**81. Unvalidated or Outdated Playbooks** –

Procedures reference obsolete systems or roles.

**82. Inadequate Cross-Role Training –**

Leads to execution failure during real events (e.g., crew briefings or system recovery).

83. **Non-Translated Lessons from Simulation Exercises** – Findings not reflected in ISMS–BCP updates or procurement.

84. **Inactive user accounts exploited for credential-based attacks.**

**85. Shared logins on line station workstations undermining traceability.**

**86. Role creep: escalation of privileges without governance.**

87. **MFA bypass or failure leading to unauthorised remote access**.

88. **VPN access granted to subcontractors using unsecured personal devices.**

89. **Inadequate cyber hygiene of external AMOs causing interface vulnerabilities.**

90. **Use of public cloud storage for maintenance data without encryption.**

91. **Badge cloning or unauthorized access to tool cribs or server rooms.**

92. **Engineers unaware of phishing/social engineering tactics.**

93. **Staff bypassing secure portals for task access due to usability constraints.**

94. **ISMS Policy Misalignment** –

ISMS objectives not aligned with organizational security strategy leading to inconsistent implementation.

95. **Incomplete Asset Inventory** –

Unidentified or unclassified digital/physical assets expose the system to unmanaged vulnerabilities.

**96. Lack of Role-Based Accountability**

Undefined responsibilities across Security, CAMO, APOPS, or Cybersecurity cause delayed responses or control failures.

**97. Insider Threat & Human Factors**

Malicious Insider Activity – Credentialed personnel misusing access for sabotage, data leakage, or theft.

**98. Negligent Insider Exposure** –

Staff unintentionally exposing credentials, misconfiguring systems, or failing to report anomalies.

99.**Unauthorized Information Disclosure** –

Internal sharing of restricted intelligence or surveillance data violating CIA principles.

100. **Training Deficiency** –

Inadequate understanding of cyber hygiene, technology use, or incident response procedures.

101. **Physical Security Risks**

Perimeter Breach – Unauthorized entry via fence breach, gate compromise, or unmonitored emergency exits.

102. **Failure of Surveillance Systems**

Downtime or data loss in CCTV coverage due to hardware failure or power outages.

**103. Credential Theft via Phishing**

Social engineering or malicious links used to capture login credentials.

104. **Access Control System Breach** – Unauthorized digital access to badge database or reader configuration.

**105. Denial of Service (DoS) on Access Systems** –

System overload affecting badge swipe validation and area lockdowns.

106. **Uncontrolled Third-Party Access – Contractors or vendors accessing restricted areas without escort or proper credentialing.**

**107. Delayed Revocation of Access** – Ex-employees or reassigned staff retaining valid credentials.

108. **Cargo Tampering or Substitution**

Unauthorized items placed in ULDs or manifest substitution.

109. **Failure of Chain-of-Custody** – Break in RFID/GPS tracking, leading to loss of location traceability.

**110. Lack of Enhanced Checks for High-Risk Cargo**

Inadequate profiling of origin or consignor history.

**111. Delayed Incident Reporting –**

Frontline staff unaware or hesitant to report anomalies.

112. **Inadequate Severity Classification –**

Underestimating impact leading to poor escalation and resource allocation.

**113. Recovery Plan Failures**

Poor testing of backup systems or unclear recovery protocols during access control failure.

Compliance & Strategic Risks

114. **Backup System Failure** –

Communication blackout during outages due to untested or degraded UPS systems.

115. **Cloud Provider Outage** –

Unavailability of third-party OFP tools due to cloud downtime, disrupting dispatch operations.

116. **Supply Chain Cyber Weakness –**

Third-party software or VPN platforms becoming vectors for malware or unauthorized access.

117. **SLAs Not Enforced** – Service delivery or availability issues not captured in supplier agreements

118. **Social Engineering Attacks on Dispatchers** –

Manipulative techniques used to extract credentials or authorize bad actors.

119. **Training Deficiencies in Incident Handling** – Inadequate preparedness for ransomware or data breach recovery.

120. **Non-Conformity with Regulation (EU) 2023/203** –

Incomplete implementation of AMC1 IS.I.OR.200(e) leading to compliance gaps.

**121. Unauthorized Access to Operational Systems**

Inadequate access controls leading to exposure of Departure Control System (DCS), Load Control, or BRS platforms to unauthorized or under-trained staff.

122. **Credential Compromise via Phishing or Spoofing**

Spoofed login portals or social engineering enabling credential harvesting, particularly in check-in and dispatch environments.

123. **Data Integrity Failures in Load Control Systems**

Altered weight and balance data due to software bugs, insider manipulation, or malware intrusion.

124. **Inadequate MFA Enforcement Across Platforms**

Absence or inconsistent application of Multi-Factor Authentication (MFA) on terminals, handhelds, or admin portals.

**125. Insider Threat from Over-Permissioned Staff**

Access privileges not aligned with operational need (e.g. admin-level access to junior baggage staff).

**126. Supply Chain Risk from Non-Compliant Vendors**

Third-party systems (CMS, catering) introducing vulnerabilities due to poor patching or non-certification.

127. **Improper Disposal of Confidential Physical Records**

Load sheets, rosters, or customs documents discarded without shredding or locked storage.