SOFEMA AVIATION SERVICES

Risk Register Considerations for a Part IS Compliant Operator, including CAMO & Maintenance

1. **Unauthorized access to DCS, BRS, W&B, and other operational platforms**
   Business Area: Passenger Services / Load Control / Baggage Handling

2. **Credential theft through phishing, spoofed portals, or social engineering**
   Business Area: Enterprise IT / Passenger Services / Dispatch

3. **Weak or reused passwords across critical systems without MFA enforcement**
   Business Area: Enterprise IT / CAMO / Maintenance

4. **Failure to revoke digital access after staff departure or contractor offboarding**
   Business Area: HR / Security / IT / CAMO

5. **Shared or orphaned third party accounts with persistent privileges**
   Business Area: Enterprise IT / CAMO / Maintenance

6. **Insider threats due to over-permissioned user roles**
   Business Area: All Business Areas

7. **Use of unsecured Wi-Fi by staff using tablets or mobile devices**
   Business Area: Ramp / Maintenance / Passenger Services

8. **Unmonitored use of portable maintenance devices without endpoint controls**
   Business Area: Maintenance / Ramp / CAMO

9. **Malware introduction via USBs or infected subcontractor devices**
   Business Area: Maintenance / Cargo / Baggage Handling

10. **Legacy systems with unsupported OS or weak encryption**
    Business Area: Passenger Services / CAMO / Baggage Handling

11. **Unencrypted or insecure data exchange with third parties**
    Business Area: Cargo / Security / Maintenance

12. **Cross-contamination between secure and non-secure devices or systems**
    Business Area: Cargo / Ramp / Security

13. **Data loss during offline tablet usage or delayed sync**
    Business Area: Load Control / CAMO / Maintenance

14. **Backup failures or lack of tested disaster recovery plans**
    Business Area: Enterprise IT / CAMO / Maintenance

15. **Unauthorized MEL/CDL edits or deferred defect tampering**
    Business Area: CAMO / Dispatch / Maintenance

16. **Lack of centralized logging and audit trails for critical systems**
    Business Area: Enterprise IT / CAMO / Dispatch

17. **Outdated or incomplete CAMO risk register not linked to SMS**
    Business Area: CAMO / Safety Management

18. **Insecure cloud hosting without formal DPA/SLA**
    Business Area: Enterprise IT / CAMO

19. **Lack of vendor ISMS governance or third-party security clauses**
    Business Area: Enterprise IT / Procurement / Legal

20. **Delayed revocation of physical access (badges, keys)**
    Business Area: Security / HR

21. **Badge cloning or tailgating leading to unauthorized access**
    Business Area: Security

22. **Tampering with CCTV/DVR or surveillance logs**
    Business Area: Security

23. **Unattended consoles in dispatch or maintenance environments**
    Business Area: Dispatch / Maintenance

24. **Use of unprotected mobile devices by security or ramp staff**
    Business Area: Security / Ramp / Aircraft Services

25. **Data leakage from unencrypted email (e.g. AMP, job cards)**
    Business Area: CAMO / Maintenance / Load Control

26. **Use of personal apps or unauthorized file-sharing platforms**
    Business Area: All Business Areas

27. **Absence of audit trail on CRS, MEL, or AMP updates**
    Business Area: CAMO / Maintenance / Dispatch

28. **Lack of asset classification or criticality prioritization**
    Business Area: Enterprise IT / CAMO / Security

29. **Mismatch between CAMO and M&E systems on aircraft status**
    Business Area: CAMO / Maintenance / Dispatch

30. **Human error during data entry (e.g. baggage tags, job cards)**
    Business Area: Baggage Handling / Load Control / Maintenance

31. **Simultaneous aircraft stand allocation due to OCC mismatch**
    Business Area: Dispatch / Ramp

32. **Conflicting or outdated load sheet versions in circulation**
    Business Area: Load Control / Dispatch

33. **Tampering with Operational Flight Plan (OFP)**
    Business Area: Dispatch / Flight Ops

34. **Insecure handover of OFP/NOTAM via hard copy or unsecured email**
    Business Area: Dispatch / Flight Ops

35. **Use of outdated or unsupported Electronic Flight Bag (EFB) apps**
    Business Area: Flight Ops / CAMO

36. **Denial of Service (DoS) targeting slot coordination or CTOT tools**
    Business Area: Dispatch / Enterprise IT

37. **Hardcoded API tokens or exposed integration keys**
    Business Area: Enterprise IT / CAMO / Dispatch

38. **Loss or corruption of technical records (electronic or physical)**
    Business Area: CAMO / Maintenance

39. **CRM or loyalty platform exploited via API vulnerabilities**
    Business Area: Passenger Services / Enterprise IT

40. **Security incident logs incomplete or tampered**
    Business Area: Enterprise IT / Security

41. **SIEM blind spots or failed detection of anomalies**
    Business Area: Enterprise IT

42. **Shadow IT usage by management or departments during crises**
    Business Area: All Business Areas

43. **Lack of integration between safety reporting and OCC systems**
    Business Area: Dispatch / Safety / OCC

44. **Delayed incident reporting or improper severity classification**
    Business Area: All Business Areas

45. **No defined ISMS incident response playbooks or protocols**
    Business Area: Enterprise IT / Safety

46. **No cross-role BCP training or simulation drills**
    Business Area: Enterprise / Safety

47. **Lack of awareness in phishing, malware, or cyber hygiene**
    Business Area: All Business Areas

48. **Role confusion during cyber incident response**
    Business Area: All Business Areas

49. **Improper disposal of physical records (e.g., customs, rosters)**
    Business Area: All Business Areas

50. **Use of outdated or manipulated calibration records or task cards**
    Business Area: Maintenance

51. **Integrity failures in tooling and component traceability systems**
    Business Area: Maintenance

52. **Insecure mobile access to ground systems (e.g. AOG tablets)**
    Business Area: Ramp / Maintenance

53. **CAMO–AMO data sync failure during maintenance release**
    Business Area: CAMO / Maintenance

54. **OPS staff editing technical records or MEL data**
    Business Area: OPS / CAMO

55. **Non-compliance with AMC1 IS.I.OR.200(e) requirements**
    Business Area: Enterprise / Governance

56. **Unsecured third-party VPN or endpoint access**
    Business Area: Enterprise IT / Maintenance / CAMO

57. **Subcontractor access without cyber hygiene enforcement**
    Business Area: Maintenance / Procurement

58. **Interface failures with airport authorities affecting coordination**
    Business Area: Ramp / Dispatch / Airport Operations

59. **Exposure of unprotected critical files on shared drives**
    Business Area: Enterprise IT / Maintenance

60. **Uncontrolled printing/duplication of job cards or CRS**
    Business Area: Maintenance / CAMO

61. **Failure of crew brief delivery due to insecure communication**
    Business Area: Dispatch / Flight Ops

62. **ATC slot data manipulation or loss of dispatch sequencing**
    Business Area: Dispatch

63. **Emergency plan failure due to poor interdepartmental execution**
    Business Area: All Business Areas

64. **Outdated ISMS policies or delayed regulatory updates**
    Business Area: Enterprise IT / Governance

65. **Failure to implement ISMS audit findings or corrections**
    Business Area: Governance / Compliance

66. **Incomplete IT asset inventory or software list**
    Business Area: Enterprise IT / CAMO

67. **Poor internal network segmentation across business units**
    Business Area: Enterprise IT / Security

68. **Simultaneous backup and production outage from shared access**
    Business Area: Enterprise IT / OCC / CAMO

69. **Version mismatch across planning, maintenance, and dispatch**
    Business Area: CAMO / Maintenance / Dispatch

70. **Chain-of-custody failure in cargo or baggage operations**
    Business Area: Cargo / Baggage Handling

71. **Misuse of trusted cargo screening channels without profiling**
    Business Area: Cargo / Security

72. **Third-party CRS submission lacking digital verification**
    Business Area: Maintenance / CAMO

73. **Lack of centralized control over aircraft software versions**
    Business Area: CAMO / AMO

74. **Use of discontinued or unsupported mobile apps in operations**
    Business Area: Flight Ops / Ramp / Maintenance

75. **Biometric access systems overridden or spoofed**
    Business Area: Security