ISMS Audit Compliance Check Sheet – EASA Part 145 AMO

(Aligned with Regulation (EU) 2023/203, EASA Part-145, MOE Part 8, and SMS integration requirements)

Section A – Governance & Documentation

Requirement: Organisation must establish and maintain an ISMS integrated with SMS.

- **ISMS Established**
  - **Check:** Confirm that the ISMM (Information Security Management Manual) exists, is controlled under MOE Part 8, and approved by the Accountable Manager.
  - **Evidence:** Latest ISMM version, approval page signed/dated, revision log.
  - **Guidance:** Audit that cyber hazards are referenced in SMS hazard logs and that CIRP links to ERP (Emergency Response Plan).
- **Quarterly ISMS Review**
  - **Check:** Verify meeting minutes exist for ISMS quarterly reviews chaired by the ISM.
  - **Evidence:** Review agenda, attendance logs, KPI dashboard, action list.
  - **Guidance:** Ensure lessons learned from incidents/audits feed back into SMS. Lack of cross-domain feedback is a non-compliance.

Section B – Policies & Risk Management

- **Policies Approved & Communicated**
  - **Check:** Ensure Information & Cyber Security, Acceptable Use, Data Classification, Supplier Security, Incident Response, and BC/DR policies exist.
  - **Evidence:** Controlled copies in ISMM; proof of distribution (bulletins, intranet, LMS logs).
  - **Guidance:** Confirm policies are less than 12 months old and signed by AM. Out-of-date or uncommunicated policies = audit finding.
- **Risk Register & Risk Treatment Plans**
  - **Check:** Review Risk Register entries for completeness (threat vector, likelihood, severity, regulatory reference).
  - **Evidence:** Register extracts, Risk Treatment Plans with owners, deadlines, KPIs.

- **Guidance:** Risks must explicitly reference aviation safety impact (e.g., compromised maintenance data leading to safety risk). Quarterly updates required.

Section C – Access Control & Authentication (MOE 8.2.2.1)

- **Multi-Factor Authentication (MFA)**
  - **Check:** Confirm MFA enforced for remote access, privileged accounts, and systems containing safety-critical/PII data.
  - **Evidence:** Identity provider policy, MFA enforcement logs, screenshots.
  - **Guidance:** Bypasses permitted only via documented break-glass with post-event review.
- **RBAC / JML Process**
  - **Check:** Confirm access requests use Form IS-01, approvals include Line Manager + ISM, and leaver accounts disabled same day.
  - **Evidence:** Sample IS-01 forms, Access Logs, account disablement timestamps.
  - **Guidance:** Any dormant accounts >30 days = major NC.
- **Privileged Access Management (PAM)**
  - **Check:** Verify admin accounts are named, session logs retained, and break-glass accounts stored in dual-control vault.
  - **Evidence:** PAM reports, vault access logs, audit trail.
  - **Guidance:** Shared admin accounts are prohibited.

Section D – Patch & Change Management (MOE 8.2.2.2)

- **Patch SLAs Met**
  - **Check:** Review patch dashboard; confirm ≥95% of critical patches applied within 14 days.
  - **Evidence:** PC-04 Patch Logs, vulnerability scan reports.
  - **Guidance:** Exceptions >90 days without mitigation = non-compliance.
- **CAB Governance**
  - **Check:** Confirm CAB reviews and approvals exist for normal/major changes.
  - **Evidence:** CAB meeting minutes, PC-01 Change Requests, rollback plans.

- **Guidance:** Verify testing in staging environment before rollout.

Section E – Backup & Recovery (MOE 8.2.2.3)

- **Backup Frequency & Retention**
  - **Check:** Ensure daily incremental, weekly full, and immutable backups for critical systems.
  - **Evidence:** BR-01 Backup Job Logs, storage system reports.
  - **Guidance:** Offsite/cloud storage must be EU-compliant and tested quarterly.
- **Restore Testing**
  - **Check:** Confirm quarterly restore tests and annual full DR exercises.
  - **Evidence:** BR-02 Restore Test Logs, DR exercise reports.
  - **Guidance:** Validate restored maintenance records against Part-145.A.55 retention obligations.

Section F – Cyber Incident Response (MOE 8.2.2.5)

- **Incident Classification & Escalation**
  - **Check:** Verify CIRP categorises incidents within 2 hours (Critical, High, Medium, Low).
  - **Evidence:** CIR-01 Incident Register, classification timestamps.
  - **Guidance:** Critical = escalation to AM + NAA immediately.
- **Regulatory Reporting**
  - **Check:** Confirm GDPR breaches reported within 72h, aviation safety incidents within NAA timeframe.
  - **Evidence:** Redacted notification letters, regulator acknowledgments.
  - **Guidance:** Absence of reporting logs = audit finding.
- **Post-Incident Review**
  - **Check:** PIRs conducted within 10 working days, corrective actions tracked.
  - **Evidence:** CIR-02 Post-Incident Reports.
  - **Guidance:** Confirm root cause updates are applied to ISMS & SMS.

Section G – Supplier Assurance (MOE 8.2.2.6)

- **Supplier Onboarding**
  - **Check:** Confirm SA-01 questionnaire completed, risk classification applied (critical/standard).
  - **Evidence:** Supplier assurance files, SA-02 Approved Supplier Register.
  - **Guidance:** Suppliers not on SA-02 register = non-compliance.
- **Contractual Security Clauses**
  - **Check:** Ensure contracts include GDPR, EU 2023/203, breach notification ≤24h, right to audit.
  - **Evidence:** Sample contracts.
  - **Guidance:** Absence of clauses in critical supplier contracts = major NC.
- **Oversight & Audits**
  - **Check:** Verify annual security audits for critical suppliers.
  - **Evidence:** SA-04 Audit Reports, NC closure evidence.
  - **Guidance:** Missing audit evidence = finding

Section H – Training & Awareness (MOE 8.2.2.7)

- **Induction & Annual Training**
  - **Check:** Confirm 100% induction before system access and ≥95% annual refresher completion.
  - **Evidence:** TR-01 Training Matrix, TR-02 Attendance Records.
  - **Guidance:** Audit random staff for training recall.
- **Role-Specific Competence**
  - **Check:** IT/Admin staff trained on patching, incident response, backups; managers trained on JML, supplier oversight.
  - **Evidence:** Specialist training certificates, competence results.
  - **Guidance:** Non-completion by key roles = non-compliance.
- **Phishing Simulations & Awareness Culture**
  - **Check:** Review phishing failure rates (≤5% target).
  - **Evidence:** TR-04 Phishing Simulation Reports.

- **Guidance:** High fail rate = observation/NC.

Section I – Business Continuity & Resilience

- **BIA & RTO/RPO Alignment**
  - **Check:** Confirm BIA completed, RTO/RPO align with maintenance obligations.
  - **Evidence:** BIA report, continuity plan.
  - **Guidance:** Missing BIA = major NC.
- **Disaster Recovery Testing**
  - **Check:** Verify last DR exercise documented, corrective actions followed.
  - **Evidence:** DR test reports, action closure logs.
  - **Guidance:** Absence of test evidence = finding.

Section J – Compliance Monitoring & Continuous Improvement

- **ISMS Audits**
  - **Check:** Confirm ISMS included in annual Compliance Monitoring Programme.
  - **Evidence:** Audit plan, audit reports.
  - **Guidance:** No audit coverage = major NC.
- **Corrective Actions**
  - **Check:** CAPs raised and tracked to closure within 10 working days.
  - **Evidence:** CAP logs, closure evidence.
  - **Guidance:** Overdue CAPs = finding.
- **KPI Reporting**
  - **Check:** Review KPIs (MFA coverage ≥99%, patch compliance ≥95%, backup success ≥99%, incident closure 100%).
  - **Evidence:** Management Review dashboards.
  - **Guidance:** Poor KPI performance without corrective actions = finding.

Audit Acceptance Criteria

- All **critical controls** (MFA, patching, backups, CIRP, supplier assurance, training, reporting) fully operational.
- **No major NCs** outstanding.

- **Minor NCs** tracked with CAPs.