Business Area ISMS Checklists

Section A – General Information (Owner: ISM / Account Manager)

Objective: Establish supplier identity, scope, governance and baseline ISMS maturity.

1. □ **Legal identity verified** (registered name, number, jurisdiction match contract). *Evidence:* Certificate of Incorporation/registry extract.
2. □ **Registered address & operating locations listed** (incl. HQ, data centers, support center's). *Evidence:* Company profile, data centre list.
3. □ **Primary ISM contact designated** (24/7 incident contact & deputy). *Evidence:* Contact sheet, on-call rota.
4. □ **ISMS certification status declared** (ISO/IEC 27001 or equivalent). *Evidence:* Valid certificate with scope & expiry.
5. □ **ISMS scope includes services for RAS Technic** (no material exclusions). *Evidence:* Statement of Applicability (SoA), scope statement.
6. □ **Information Security Policy approved within 12 months**. *Evidence:* Policy with approval date/version control.
7. □ **Governance model defined** (roles, committees, reporting lines). *Evidence:* Org chart, IS governance charter.
8. □ **Risk management process in place** (method, cadence, risk register). *Evidence:* Extract of risk register with recent entries.
9. □ **Mandatory security training for all staff** (incl. contractors) within past 12 months. *Evidence:* LMS report, syllabus.
10. □ **Role-based training for elevated roles** (admins, developers, support). *Evidence:* Training matrix, attendance.
11. □ **Asset inventory maintained** (information assets, systems, owners). *Evidence:* Asset register sample.
12. □ **Data processing role clarified** (Controller/Processor; joint processing, if any). *Evidence:* DPIA/RoPA entries.
    - **DPIA – Data Protection Impact Assessment - Definition:** A structured risk assessment required under GDPR (Art. 35).
    - **Purpose:** To evaluate and mitigate risks to the rights and freedoms of individuals when processing personal data, especially if processing is high-risk (e.g., large-scale monitoring, sensitive data, cross-border transfers).

      Evidence in context:

    - A completed **DPIA report** showing that the supplier has assessed the risks of how they handle AMO Technic data.
    - The report should include scope, necessity/proportionality, risks identified, and mitigations applied.

- **Why it matters:** Demonstrates that the supplier has thought through privacy risks before starting processing, reducing exposure for RAS Technic.

- **RoPA – Record of Processing Activities**

- **Definition:** A GDPR requirement under Art. 30 for both controllers and processors.
- **Purpose:** To maintain a central register describing all personal data processing operations carried out by an organisation.
- **Content typically includes:**
- Categories of data subjects and personal data.
- Purposes of processing.
- Recipients of data (including third countries).
- Retention periods.
- Technical and organisational measures (security).

Evidence in context:
- A supplier providing a **RoPA entry** relevant to AMO Technic data.
- This shows exactly how, where, and why your data is processed, and ensures GDPR accountability.

13. □ **Locations & data residency constraints disclosed** (EEA/third-country transfers). *Evidence:* RoPA, transfer mapping.
14. □ **Change notification process** for material changes impacting security. *Evidence:* Change control procedure.
15. □ **Insurance coverage** (cyber/tech E&O) meets contractual minimums. *Evidence:* Insurance certificate.
16. □ **Ethics/ABAC policy** (anti-bribery/anti-corruption) published & acknowledged. *Evidence:* Policy & attestations.
17. □ **Business ownership & key principals disclosed** (PEP/sanctions screened). *Evidence:* Ownership statement, screening record.
18. □ **Third-party certifications register maintained** (current, no critical non-conformities open). *Evidence:* Cert register, NC closure evidence.

Acceptance: All mandatory items 1–6 and 8–10 must be satisfied; any gap requires corrective action with due date.

Section B – Contractual & Legal Compliance (Owner: Legal/Procurement)
Objective: Ensure contracts embed ISMS obligations, regulatory alignment, and enforceable rights.

1. □ **Security & confidentiality clauses** aligned to EU 2023/203 & ISO 27001. *Evidence:* Executed contract/SOW.

2. □ **24-hour breach notification** defined with contact method/escalation. *Evidence:* Clause excerpt.
3. □ **Right to audit & evidence disclosure** (incl. third-party reports) granted. *Evidence:* Clause excerpt.
4. □ **GDPR DPA executed** (roles defined; controller/processor; joint controller, if applicable). *Evidence:* Signed DPA.
5. □ **International transfer mechanism** in place (SCCs/IDTA/BCRs). *Evidence:* Signed SCCs, TIAs.
6. □ **Sub-processor approval & flow-down** obligations defined. *Evidence:* Sub-processor list & contract flow-down.
7. □ **Regulatory compliance** obligations (EASA Part-145/Part-CAMO references where applicable). *Evidence:* Contract clause.
8. □ **Change control** for material security changes (advance notice & review). *Evidence:* Change clause.
9. □ **Termination for cause** for material security non-compliance/remediation failure. *Evidence:* Termination clause.
10. □ **Data retention & secure deletion** defined (incl. backups & timelines). *Evidence:* Schedule.
11. □ **Records & audit trail retention** period meets regulatory needs. *Evidence:* Contract schedule.
12. □ **Liability/apportionment** suitable for data breach/cyber events. *Evidence:* Liability clause.
13. □ **Incident cooperation & forensics access** defined. *Evidence:* Contract language.
14. □ **Notification of adverse events** (law enforcement/regulator notices, sanctions). *Evidence:* Clause.
15. □ **Insurance requirements** specified (limits/types). *Evidence:* Contract schedule.
16. □ **IP escrow/continuity** for critical software (if applicable). *Evidence:* Escrow agreement.
17. □ **Confidentiality survival** period adequate post-termination. *Evidence:* Clause.
18. □ **Audit remediation timelines** and corrective action plans mandated. *Evidence:* Clause/SLA.
19. □ **Jurisdiction/governing law** appropriate and consistent. *Evidence:* Contract.
20. □ **Anti-bribery /AML (Anti-Money Laundering) & sanctions compliance** warranted. *Evidence:* Warranties.

Acceptance: Items 1–9, 12, 15, 18 are mandatory for critical suppliers; deviations require risk acceptance by ISM & Legal.

Section C – Access Control (Owner: IAM Lead)

Note - When the Owner: IAM Lead is listed, it means that the responsible person for verifying compliance in that section is the **Identity and Access Management** Lead (or equivalent role in the supplier's organisation).
In smaller organisations, this responsibility might sit with the IT Manager, Security Manager, or outsourced MSP, but in a mature ISMS the IAM Lead is a dedicated function.

Typical Responsibilities of an IAM Lead:

- **Identity lifecycle management** – making sure user accounts are created, modified, and deleted promptly (Joiner–Mover–Leaver process).
- **Authentication controls** – enforcing strong authentication (e.g., multi-factor authentication, single sign-on).
- **Authorization controls** – ensuring that access rights follow the principle of least privilege and separation of duties.
- **Privileged Access Management (PAM)** – controlling and monitoring admin and elevated accounts.
- **Access recertification** – conducting regular reviews of user rights to confirm ongoing need.
- **Policy enforcement** – making sure identity and access policies align with ISMS requirements, aviation regulatory obligations (e.g., EASA Part-145 digital record access), and contractual commitments.
- **Audit & evidence** – providing logs and reports to internal/external auditors and regulators.

Objective: Enforce least privilege, strong authentication and timely lifecycle control.

1. □ **MFA (Multi-Factor Authentication) enforced** for remote, admin and privileged accounts. *Evidence:* IdP policies, screenshots.
2. □ **SSO via managed IdP** with conditional access where possible. *Evidence:* Architecture diagram.
    - **SSO (Single Sign-On)** A method that lets a user log in once and gain access to multiple systems or applications without needing to re-enter credentials each time.
    - **IdP (Identity Provider) Meaning:** The central system/service that manages digital identities and handles authentication requests for applications.
3. □ **Joiner-Mover-Leaver (JML)** process with documented SLAs (provision ≤24h; revoke ≤24h). *Evidence:* Procedure & logs.
4. □ **Access recertification** cadence defined (quarterly for critical, semi-annual for others). *Evidence:* Review reports.

5. □ **RBAC/SOD** implemented for critical systems (no conflicting roles). *Evidence:* Role matrix.
   RBAC – Role-Based Access Control - access rights are granted based on roles within an organisation rather than individual assignments -
   SOD – Segregation of Duties - Critical tasks are split between different people or roles so no single individual can both perform and approve the same sensitive activity.
6. □ **Privileged Access Management (PAM)** in place (vaulting, session recording). *Evidence:* PAM config/report.
7. □ **Service accounts** uniquely owned, non-interactive, rotated & monitored. *Evidence:* Inventory & rotation logs.
8. □ **Password policy** aligned to NIST/industry guidance (length, reuse, lockout). *Evidence:* Policy extract/IdP settings.
9. □ **Network/VPN access** restricted to managed devices with posture checks. *Evidence:* NAC/MDM config.
10. □ **Third-party access** segregated (least privilege, time-bound, separate tenants where feasible). *Evidence:* Access lists.
11. □ **Administrative activity logging** enabled & reviewed. *Evidence:* SIEM dashboards.
12. □ **Break-glass procedures** defined and tested. *Evidence:* Runbook & test record.
13. □ **Physical access** to hosting locations controlled & logged. *Evidence:* Badge logs/cert attestations.
14. □ **Backup/restore admin access** tightly controlled & segregated. *Evidence:* Access list.
15. □ **API keys/Secrets management** centralized & rotated. *Evidence:* Secrets manager logs.
16. □ **Account dormancy** auto-disable thresholds defined (e.g., 30/60 days). *Evidence:* IdP rules.
17. □ **Contractor access** time-boxed with auto-expiry. *Evidence:* Tickets/audit log.
18. □ **Periodic access spot-checks** by asset owners. *Evidence:* Sample approvals.

Acceptance: No critical exceptions on items 1–7 and 11; medium gaps require compensating controls.

Section D – Data Protection & Encryption (Owner: DPO / Data Security Lead)
Objective: Protect confidentiality/integrity of data across lifecycle and meet GDPR obligations.

1. □ **TLS 1.2+ enforced** for all data in transit (with HSTS where applicable). *Evidence:* Config scan, policy.
   TLS (Transport Layer Security): The cryptographic protocol used to secure data as it moves between systems (e.g., between a browser and a web server, or between two APIs). It's the successor to SSL

1.2+: Means the minimum acceptable version is TLS 1.2 (released 2008) or higher (e.g., TLS 1.3, released 2018) - A web security policy mechanism that forces browsers to connect only via HTTPS (TLS-secured)

2. □ **Encryption at rest** for databases, file stores, backups (AES-256 or equivalent). *Evidence:* Platform settings.
3. □ **Key management** via KMS/HSM; role separation for key custodians. *Evidence:* KMS policy.
    - **KMS** – Key Management System - used to generate, distribute, rotate, store, and revoke cryptographic keys.
    - **HSM –** Hardware Security Module - A dedicated physical device designed to store and protect cryptographic keys securely.
4. □ **Key rotation** policy & evidence (e.g., 12-month cycle). *Evidence:* Rotation logs.
5. □ **Data classification policy** (Public/Internal/Confidential/Restricted) implemented. *Evidence:* Policy, labels.
6. □ **Data minimisation** & purpose limitation practiced. *Evidence:* DPIA/RoPA extracts.
   DPIA – Data Protection Impact Assessment
   RoPA – Record of Processing Activities
7. □ **Data retention schedules** defined & enforced (incl. backups). *Evidence:* Retention policy, purge logs.
8. □ **Secure disposal** methods (crypto-erase/shred; certificates of destruction). *Evidence:* Destruction certs.
9. □ **MDM controls** for endpoints (disk encryption, screen lock, remote wipe). *Evidence:* MDM policy/report.
    - MDM – Mobile Device Management - policies, software, and tools used to control and secure endpoints such as:
        - Laptops / Tablets / Smartphones / Any portable device accessing company systems
10. □ **Secure file transfer** approved channels only (SFTP/HTTPS; no personal email). *Evidence:* Policy & tooling.
11. □ **Removable media** restricted and encrypted if permitted. *Evidence:* Policy & logs.
12. □ **Certificate lifecycle** managed (expiry alerts, inventory). *Evidence:* PKI inventory.
    Public Key Infrastructure (PKI) is the framework of policies, hardware, software, and procedures needed to manage:
    - **Digital certificates** (used for authentication, signing, encryption).
    - **Public and private keys** (used in cryptography).
13. □ **Privacy by design** evidenced in change/projects. *Evidence:* DPIA templates, sign-offs.

14. □ **RoPA maintained** with processing purposes, categories, recipients, locations. *Evidence:* RoPA export.
15. □ **Third-country transfer TIAs** performed where applicable. *Evidence:* TIA documents.
    TIA – Transfer Impact Assessment
16. □ **Access to production data** restricted & logged (no live data in lower envs). *Evidence:* Logs & policy.
17. □ **Backup encryption & immutability** confirmed. *Evidence:* Backup solution settings.
18. □ **Data subject rights** process tested (access/erasure/rectification). *Evidence:* Ticket examples.
19. □ **Breach assessment** rule set includes GDPR & contractual thresholds. *Evidence:* IR policy.

Acceptance: Items 1–4, 5, 7, 15, 18, 20 are mandatory for critical suppliers.

Section E – Vulnerability & Patch Management (Owner: SecOps / Platform Lead)
Objective: Timely discovery, risk assessment, and remediation of vulnerabilities.

1. □ **Patch SLAs** defined (e.g., Critical ≤7 days; High ≤30). *Evidence:* Policy.
2. □ **OS & platform updates** tracked with compliance reports. *Evidence:* Patch dashboard.
3. □ **Third-party software** patching covered (browsers, runtimes, libraries). *Evidence:* Tooling reports.
4. □ **Emergency patch process** for zero-days with change control. *Evidence:* Runbook & examples.
5. □ **Authenticated vulnerability scanning** of servers/endpoints. *Evidence:* Recent scan reports.
6. □ **Web app/API scanning** (DAST) and dependency checks (SCA). *Evidence:* Reports.
7. **API = Application Programming Interface -** An API is a set of rules, protocols, and tools that allows different software applications to communicate with each other.
8. □ **Cloud configuration scanning** against benchmarks (e.g., CIS). *Evidence:* CSPM dashboards.
9. □ **CVSS-based risk triage** with business context. *Evidence:* Triage records.
10. □ **Remediation tracking** via tickets to closure (aging monitored). *Evidence:* Ticket metrics.
11. □ **Exception management** with compensating controls & expiry. *Evidence:* Exceptions log.
12. □ **Configuration baselines** defined & measured. *Evidence:* Baseline docs/audit.
13. □ **EDR/AV** deployed with up-to-date signatures & alerting. *Evidence:* EDR console.
14. □ **Firmware/BIOS updates** policy. *Evidence:* Procedure & sample.

15. □ **Pen test at least annually** for critical scope with retest. *Evidence:* Report & fix verification.
16. □ **Threat intel ingestion** & vendor advisories tracked. *Evidence:* Feed list, action logs.
17. □ **SBOM availability** for supplied software (where applicable). *Evidence:* SBOM artifact.
18. □ **Exposure management metrics** (MTTR, backlog, SLA adherence). *Evidence:* KPI report.
19. □ **Secure configuration of build pipelines** (if software delivered). *Evidence:* CI/CD controls.

Acceptance: Critical gaps in 1, 5–9, 12, 14 require immediate plan and periodic reporting.

Section F – Incident Management (Owner: IR Lead / ISM)

Objective: Rapid detection, response, notification, and recovery aligned with EU 2023/203.

1. □ **IR Plan** current, approved, version-controlled. *Evidence:* Plan document.
   Incident Response (IR) Plan
2. □ **RACI** for incidents defined (incl. legal, comms, ops). *Evidence:* RACI matrix.
   RACI – Identification
   R – Responsible - The person(s) who actually perform the task or activity.

   A – Accountable The person ultimately answerable for the correct completion of the task.
   C – Consulted - People whose input is required before a decision or action can be taken. Involves two-way communication.
   I – Informed - People who must be kept updated about progress or decisions. Involves one-way communication.
3. □ **24/7 escalation** paths & contact tree tested. *Evidence:* Call tree test record.
4. □ **Detection capabilities** (SIEM, EDR, IDS) with tuned use cases. *Evidence:* Alert catalog.
   SIEM – Security Information and Event Management
   EDR – Endpoint Detection and Response
   IDS – Intrusion Detection System
5. □ **Severity classification & thresholds** defined, including breach criteria. *Evidence:* IR taxonomy.
6. □ **Customer notification workflow** meets 24h requirement. *Evidence:* SOP & past examples.
7. □ **Forensics & evidence handling** (chain of custody). *Evidence:* Procedure & case logs.
8. □ **Tabletop exercises** at least annually with lessons learned tracked. *Evidence:* Exercise report.

9. □ **Runbooks/playbooks** for common scenarios (ransomware, BEC, DDoS, insider). *Evidence:* Playbooks.
   BEC – Business Email Compromise
   DDoS – Distributed Denial of Service

10. □ **Backup isolation & restore verification** integrated into IR. *Evidence:* Test records.
11. □ **Third-party & regulator coordination** process defined. *Evidence:* SOP.
12. □ **Post-incident review (PIR)** within 10 business days. *Evidence:* PIR reports.
13. □ **Metrics/KPIs** (MTTD, MTTR, notification timeliness) monitored. *Evidence:* Dashboard.
    MTTD – Mean Time to Detect
    MTTR – Mean Time to Respond / Recover
14. □ **Evidence of recent incidents** and corrective actions (if any) provided. *Evidence:* Redacted case summaries.
15. □ **Crisis communications plan** (exec/PR alignment). *Evidence:* Plan & templates.
16. □ **Legal counsel access** pre-arranged (privilege considerations). *Evidence:* Engagement letter.
17. □ **Malware handling & quarantine** procedures. *Evidence:* SOP & EDR policy.
    EDR – Endpoint Detection and Response - is a cybersecurity solution installed on endpoints (computers, laptops, servers, sometimes mobile devices) to detect, investigate, and respond to suspicious activity

18. □ **Insider incident** detection & response controls. *Evidence:* UEBA rules, SOP.
    UEBA – User and Entity Behavior Analytics
    Examples of UEBA rules:
    User logs in from two countries within one hour.
    Multiple failed login attempts followed by a successful one.
    Privileged account used outside of normal working hours.

Acceptance: Items 1–6, 8, 10, 12, 13 must be established with evidence.

Section G – Business Continuity & Resilience (Owner: BCP/DR Manager)

Objective: Maintain continuity for services supporting AMO Technic within agreed RTO/RPO.

1. □ **Business Impact Analysis (BIA)** completed & current. *Evidence:* BIA report.
2. □ **RTO/RPO** set for critical systems and align to contract. *Evidence:* BCP schedule.
3. □ **Documented BCP/DRP** with named owners. *Evidence:* Plans & approvals.
   RPO – Recovery Point Objective - Amount of data loss, measured in time between the last backup and the incident.

RTO – Recovery Time Objective - The maximum acceptable time a system or service can be down after a disruption before it must be restored.
BCP (Business Continuity Plan): Covers how RAS Technic continues operations during disruption (alternate sites, manual workarounds, staff relocation).
DRP (Disaster Recovery Plan): A subset of BCP, focused on restoring IT systems and data.

4. □ **Dependency mapping** (people, tech, suppliers, facilities). *Evidence:* Dependency register.
5. □ **Backup strategy** (3-2-1; immutable copies). *Evidence:* Backup design.
6. □ **Restore testing cadence** with sampled success criteria. *Evidence:* Test logs.
7. □ **Most recent DR test** results & follow-ups. *Evidence:* Report & actions.
8. □ **Capacity & scaling plans** for peak demand/failover. *Evidence:* Capacity plan.
9. □ **Single points of failure** identified and mitigations planned. *Evidence:* Risk register.
10. □ **Staff continuity** (cross-training, vendor support, call-out). *Evidence:* Rota & skills matrix.
11. □ **Pandemic/geo-risk scenarios** covered (remote ops viability). *Evidence:* Scenario plans.
12. □ **Power/cooling resilience** (UPS, generator contracts). *Evidence:* Facilities attestations.
13. □ **Third-party/supplier continuity** (upstream dependencies assessed). *Evidence:* Supplier BCP attestations.
14. □ **Data integrity checks** post-restore (hash/QA steps). *Evidence:* Procedure.
15. □ **BCP awareness & training** for key roles. *Evidence:* Attendance.
16. □ **Communications plan** for incidents & status updates to customers. *Evidence:* Templates.
17. □ **Exit & transition plan** to alternative provider. *Evidence:* Exit plan.

Acceptance: Items 1–3, 6–8, 14, 18 required for critical services.

Section H – External Assurance & Oversight (Owner: Assurance & Audit Liaison)
Objective: Obtain independent assurance of control effectiveness and continuous improvement.

1. □ **ISO/IEC 27001 certificate** current; scope aligns; auditor accredited. *Evidence:* Cert & scope.
2. □ **Last surveillance/recert audit** with NCs closed on time. *Evidence:* Audit report & closure.
3. □ **SOC 2 Type II (or equivalent)** available for relevant scope. *Evidence:* SOC report & bridge letters.
4. □ **Annual penetration test** by recognised provider (CREST/Tiger or equivalent). *Evidence:* Report & retest letter.
5. □ **Vulnerability disclosure policy** (VDP) published, bug bounty where applicable. *Evidence:* VDP link.
6. □ **Insurance – Cyber liability** adequate and current. *Evidence:* Policy schedule.

7. □ **Security ratings** monitored & acceptable (e.g., BitSight/SecurityScorecard). *Evidence:* Score snapshot.
8. □ **Customer audit support** defined (NDA, scheduling, data room). *Evidence:* SOP.
9. □ **Change notification for control downgrades** established. *Evidence:* Policy clause.
10. □ **Third-party attestations mapping** to TR-01 controls available. *Evidence:* Control mapping.
11. □ **Frequency of independent audits** (≥ annually for critical scope). *Evidence:* Audit calendar.
12. □ **Open findings backlog** tracked with target dates. *Evidence:* Findings log.
13. □ **Internal audit programme** complements external assurance. *Evidence:* IA plan & report.
14. □ **Software supply-chain attestations** (SBOM, SLSA level where applicable). *Evidence:* Attestations.
15. □ **Responsible disclosure process** integrates into IR & patching. *Evidence:* SOP linkage.
16. □ **Pen test scope coverage** includes external, internal, app & API. *Evidence:* Scope letter.
17. □ **Compliance statements** for sectoral regulations (aviation, where relevant). *Evidence:* Statements.
18. □ **Historic RAS audit actions** closed or on track. *Evidence:* Action tracker.

Acceptance: Items 1–4, 8–10, 12 are baseline for high-risk suppliers.

Section I – Subcontracting (Owner: Vendor Management Lead)
Objective: Manage security risk from sub-processors and fourth parties; ensure contractual flow-down.

1. □ **Complete sub-processor register** (service, location, data types). *Evidence:* Current list.
2. □ **Risk classification** of each sub-processor (Critical/Standard/Low). *Evidence:* Risk register.
3. □ **DPA & security clauses** flowed down to subs. *Evidence:* Sample contracts.
4. □ **Advance notification & approval** process for adding/changes to subs. *Evidence:* SOP & examples.
5. □ **Breach notification SLA** for subs (≤24h) contractually required. *Evidence:* Clause excerpts.
6. □ **Right to audit subs** (directly or via supplier) ensured. *Evidence:* Contract clause.
7. □ **Geographic processing locations** disclosed; transfer mechanisms valid. *Evidence:* SCCs/TIAs.
8. □ **Sub-processor assurance** (certs, SOC, pen tests) collected & reviewed annually. *Evidence:* Reports.

9. □ **Technical segregation** between supplier and subs (network/tenant). *Evidence:* Architecture.
10. □ **Least-privilege access** for subs; time-bound credentials. *Evidence:* Access logs.
11. □ **Exit/transition plans** for sub failure or replacement. *Evidence:* Plan documents.
12. □ **Data return/deletion** obligations on sub termination. *Evidence:* Contract clauses.
13. □ **Concentration risk** assessed (single points of failure). *Evidence:* Risk analysis.
14. □ **Fourth-party dependencies** identified (material exposures). *Evidence:* Mapping.
15. □ **BCP/DR attestations from subs** obtained & reviewed. *Evidence:* Attestations.
16. □ **Security incident drill** including subs performed periodically. *Evidence:* Exercise report.
17. □ **Device/endpoint compliance** for sub access (MDM/EDR). *Evidence:* Policy/attestations.
18. □ **Change management** captures sub changes and impact assessments. *Evidence:* CAB minutes.
19. □ **Performance & SLA monitoring** of subs (incl. security KPIs). *Evidence:* Reports.
20. □ **Financial health & viability** checks on critical subs. *Evidence:* Credit/financial reports.

Acceptance: Items 1–8, 10–12, 15 are mandatory for any sub processing personal or regulated maintenance data.

Scoring & Closure (Internal ISM Use)

- Score each control: **2 = Compliant, 1 = Partial, 0 = Non-compliant**.
- Compute % compliance and risk level: **Low >80%**, **Medium 60–80%**, **High <60%**.
- Record corrective actions, owners, and due dates in the Supplier Assurance Register.