Expected Documentation for a SaaS Use-Case

The following is the documentation and evidence I would expect a SaaS organisation preparing for ISO/IEC 27001:2022 certification to be able to share for the pre-audit. Items marked with clause or control references map to ISO/IEC 27001:2022. Not every item is mandatory in every case. Annex A controls apply only if marked "applicable" in the Statement of Applicability, but gaps against this list are a useful readiness indicator.

A. Core ISMS documents (Clauses 4–10)

- ☐ ISMS scope statement *(Clause 4.3)*
- ☐ Information security policy *(Clause 5.2)*
- ☐ Roles, responsibilities and authorities for information security *(Clause 5.3)*
- ☐ Risk assessment methodology, incl. risk acceptance criteria *(Clause 6.1.2)*
- ☐ Risk assessment results / risk register *(Clauses 6.1.2, 8.2)*
- ☐ Risk treatment plan, approved by risk owners *(Clauses 6.1.3, 8.3)*
- ☐ Statement of Applicability (SoA) *(Clause 6.1.3 d))*
- ☐ Information security objectives and plans to achieve them *(Clause 6.2)*
- ☐ Competence and training records; awareness evidence *(Clauses 7.2, 7.3)*
- ☐ Document control approach for ISMS documented information *(Clause 7.5)*
- ☐ Monitoring and measurement results for the ISMS *(Clause 9.1)*
- ☐ Internal audit program and most recent internal audit report *(Clause 9.2)*
- ☐ Management review minutes *(Clause 9.3)*
- ☐ Nonconformity and corrective action log *(Clause 10.2)*

B. Policies & organisational controls

- ☐ Topic-specific policies (acceptable use, access control, cryptography, backup, etc.) *(A.5.1)*
- ☐ Asset inventory with designated owners, incl. information assets and cloud services *(A.5.9)*
- ☐ Information classification and labelling scheme *(A.5.12, A.5.13)*
- ☐ Access control policy and user access provisioning / deprovisioning process *(A.5.15–A.5.18)*
- ☐ Supplier security policy and register of suppliers / sub-processors *(A.5.19–A.5.22)*
- ☐ Cloud services acquisition and exit requirements *(A.5.23)*
- ☐ Incident management procedure and incident log *(A.5.24–A.5.27)*
- ☐ Business continuity / ICT readiness plans and test evidence *(A.5.29, A.5.30)*
- ☐ Register of legal, statutory, regulatory and contractual requirements *(A.5.31)*
- ☐ Records of processing / privacy documentation (GDPR / FADP) *(A.5.34)*

C. People & physical controls

- ☐ Screening / background check practice for new hires *(A.6.1)*
- ☐ Employment contracts or annexes covering security responsibilities and confidentiality *(A.6.2, A.6.6)*
- ☐ Security awareness training program and completion records *(A.6.3)*
- ☐ Remote working rules *(A.6.7)*
- ☐ Physical security arrangements for offices (if any) — often lightweight for cloud-native SaaS *(A.7.1–A.7.4)*

D. Technology & SaaS-specific evidence

- ☐ Endpoint / device management standard (laptops, MDM, disk encryption) *(A.8.1)*
- ☐ Privileged access management approach (admin accounts, cloud root accounts) *(A.8.2)*
- ☐ MFA / secure authentication configuration evidence *(A.8.5)*
- ☐ Malware protection and vulnerability management process, incl. patching and scanning *(A.8.7, A.8.8)*
- ☐ Configuration management / infrastructure-as-code baseline *(A.8.9)*
- ☐ Data deletion and retention rules, incl. customer data on contract exit *(A.8.10)*
- ☐ Backup policy and restore test evidence *(A.8.13)*
- ☐ Redundancy / availability architecture description (multi-AZ, failover) *(A.8.14)*
- ☐ Logging and monitoring setup; log protection and alerting *(A.8.15, A.8.16)*
- ☐ Network security architecture diagram, segregation of environments *(A.8.20–A.8.22, A.8.31)*
- ☐ Cryptography / encryption standard (data at rest, in transit, key management) *(A.8.24)*
- ☐ Secure development lifecycle policy, incl. code review and secure coding rules *(A.8.25–A.8.28)*
- ☐ Security testing evidence (penetration test report, vulnerability scan results) *(A.8.29)*
- ☐ Change management process for production releases *(A.8.32)*
- ☐ Test data handling rules *(A.8.33)*

E. Cloud & third-party assurance

- ☐ Cloud provider agreements and shared-responsibility documentation (e.g. AWS/Azure/GCP) *(A.5.21, A.5.23)*
- ☐ Sub-processor list and data processing agreements (DPAs) *(A.5.20, A.5.34)*
- ☐ Third-party assurance reports collected from providers (SOC 2, ISO 27001 certificates) *(A.5.22)*
- ☐ Customer-facing security documentation (trust page, security whitepaper) — if it exists

---

Note: if several items in Sections A and B do not yet exist, in particular the risk assessment, Statement of Applicability, internal audit and management review, the recommended next step is a gap analysis and implementation phase rather than a pre-audit.