Building an ISO 27001-Compliant Cyber Security Program: Getting Started

with Marc Menninger

Mandatory Documents and Records Required by ISO/IEC 27001:2013

- Scope of the ISMS (Clause 4.3)
- Information security policy and objectives (Clauses 5.2 and 6.2)
- Risk assessment and risk treatment methodology (Clause 6.1.2)
- Statement of Applicability (Clause 6.1.3 d)
- Risk treatment plan (Clauses 6.1.3 e and 6.2)
- Risk assessment report (Clause 8.2)
- Definition of security roles and responsibilities (Clauses A.7.1.2 and A.13.2.4)
- Inventory of assets (Clause A.8.1.1)
- Acceptable use of assets (Clause A.8.1.3)
- Access control policy (Clause A.9.1.1)
- Policy on the use of cryptographic controls (Clause A.10.1.1)
- Key management policy (Clause A.10.1.2)
- Operating procedures for IT management (Clause A.12.1.1)
- Secure system engineering principles (Clause A.14.2.5)
- Supplier security policy (Clause A.15.1.1)
- Incident management procedure (Clause A.16.1.5)
- Business continuity procedures (Clause A.17.1.2)
- Statutory, regulatory, and contractual requirements (Clause A.18.1.1)

And here are the mandatory records:

- Records of training, skills, experience, and qualifications (Clause 7.2)
- Monitoring and measurement results (Clause 9.1)
- Internal audit program (Clause 9.2)
- Results of internal audits (Clause 9.2)
- Results of the management review (Clause 9.3)
- Results of corrective actions (Clause 10.1)
- Logs of user activities, exceptions, and security events (Clauses A.12.4.1 and A.12.4.3)

Non-mandatory documents

There are numerous non-mandatory documents that can be used for ISO 27001 implementation, especially for the security controls from Annex A. However, I find these non-mandatory documents to be most commonly used:

- Statement of management commitment to security (Clause 5.1)
- Procedure for document control (Clause 7.5)
- Controls for managing records (Clause 7.5)
- Procedure for internal audit (Clause 9.2)
- Procedure for corrective action (Clause 10.1)
- Bring your own device (BYOD) policy (Clause A.6.2.1)
- Mobile device and teleworking policy (Clause A.6.2.1)
- Information classification policy (Clauses A.8.2.1, A.8.2.2, and A.8.2.3)
- Password policy (Clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)
- Disposal and destruction policy (Clauses A.8.3.2 and A.11.2.7)
- Procedures for working in secure areas (Clause A.11.1.5)
- Clear desk and clear screen policy (Clause A.11.2.9)
- Change management policy (Clauses A.12.1.2 and A.14.2.4)
- Backup policy (Clause A.12.3.1)
- Information transfer policy (Clauses A.13.2.1, A.13.2.2, and A.13.2.3)
- Business impact analysis (Clause A.17.1.1)
- Exercising and testing plan (Clause A.17.1.3)
- Maintenance and review plan (Clause A.17.1.3)
- Business continuity strategy (Clause A.17.2.1)