CONCEPT

ISO 27001 Annex A Controls: Implementation, Statement of Applicability and Internal Audit

ISO 27001 Annex A Controls: Implementation, Statement of Applicability and Internal Audit

Technical depth: Practitioner · **Practical mode:** Case study

Introduction

Many organisations hold an ISO/IEC 27001 certificate or plan to, yet their controls exist mainly on paper. The Statement of Applicability is copied from a template, control owners cannot show evidence, and internal audits test documents rather than whether controls work. This Core Concept course takes participants through the 2022 Annex A control set, from selecting and implementing controls to planning audits, testing evidence and writing findings. Case material comes from several sectors, and participants leave with a Control Implementation and Audit Pack for their own organisation.

Course Objectives

- Determine the ISMS scope and identify control gaps against ISO/IEC 27001:2022 Annex A
- Apply ISO/IEC 27002:2022 guidance and ISO/IEC 27005:2022 risk treatment to select and justify controls
- Implement organisational, people, physical and technological controls with defined owners and evidence
- Plan and conduct a risk-based internal audit of controls in line with ISO 19011:2018 and ISO/IEC 27007:2020
- Grade nonconformities, write audit findings and verify corrective actions
- Build a Control Implementation and Audit Pack ready for management review

Target Audience

- ISMS implementers and coordinators responsible for putting controls in place
- Control owners in IT, facilities, HR and procurement who must produce evidence
- Internal auditors and assurance specialists testing information security controls
- Compliance officers maintaining control registers and audit readiness
- IT security analysts supporting certification and surveillance audits

Course Outline

Day 1: The ISMS and the 2022 Control Set

- ISO/IEC 27001:2022 and Amendment 1:2024 Requirements Overview
- ISMS Scope Statement and Interested Parties Analysis
- Annex A Structure: 93 Controls in Four Themes
- Control Gap Assessment Against Annex A
- Mapping from the 2013 Control Set to the 2022 Control Set

Day 2: Implementation and Audit Standards

- ISO/IEC 27002:2022 Control Attributes and Implementation Guidance
- ISO/IEC 27003:2017 ISMS Implementation Guidance
- Risk Treatment Plan Linkage with ISO/IEC 27005:2022
- ISO 19011:2018 Audit Principles and Audit Programme Management
- ISO/IEC 27007:2020 ISMS Audits and ISO/IEC TS 27008:2019 Control Assessment

Day 3: Implementing the Controls

- Statement of Applicability Drafting with Inclusion and Exclusion Justifications
- Organisational Controls: Topic-Specific Policies, Asset Inventory and Supplier Agreements
- People Controls: Screening, Awareness and Remote Working
- Physical Controls: Secure Areas, Equipment Protection and Clear Desk
- Technological Controls: Access Rights, Logging, Configuration and Backup

Day 4: Auditing the Controls

- Internal Audit Plan and Risk-Based Audit Checklist Design
- Audit Evidence Techniques: Interview, Observation, Sampling and Re-performance
- Testing New 2022 Controls: Threat Intelligence, Cloud Services, Data Masking and Web Filtering
- Nonconformity Grading and Audit Finding Statements
- Corrective Action Verification and Root Cause Analysis with the 5 Whys

Day 5: Case Work and the Control Implementation and Audit Pack

- SaaS Provider Case Study: Evidence File Review
- Hospital Case Study: Access Control and Logging Audit
- Statement of Applicability and Control Implementation Plan for an Own Organisation
- Internal Audit Programme and Control Test Script Build
- Audit Findings Presentation and Peer Challenge

Skills You Will Gain

- ISMS Scoping
- Control Selection and Justification
- Control Implementation Planning
- Audit Evidence Evaluation
- Control Testing
- Audit Finding Writing
- Corrective Action Follow-Up

Why Attend This Course

- Return with a Control Implementation and Audit Pack that reflects your own scope, risks and controls
- Replace template-driven control statements with evidence that stands up to external audit
- Recognise the control areas where certification and surveillance audits most often raise findings
- Exchange practical audit experience with peers from other sectors and countries

Conclusion

An ISMS is only as strong as the controls that operate day to day and the audits that test them honestly. This course moves from the 2022 control set and the standards that guide its implementation and audit, through putting organisational, people, physical and technological controls in place, to planning audits, testing evidence and grading findings. The final day produces a Control Implementation and Audit Pack that participants take back to their organisation, ready to support management review and the next audit cycle.