ISO/IEC 27001:2022 Training Syllabus

Module 1: Introduction to ISO/IEC 27001:2022 & Key Updates

Objective: Understand the fundamentals and changes from ISO 27001:2013 to 2022.
Topics:

- Overview of Information Security Management System (ISMS)
- Purpose, scope, and benefits of ISO 27001
- Structure of ISO standards (HLS – High Level Structure)
- Key changes in the 2022 revision (e.g., control reorganization, attributes)
- Mapping of ISO 27001:2022 to ISO 27002:2022

Module 2: ISMS Context, Leadership & Planning

Objective: Understand the core clauses and foundational structure of ISMS. **Clause 4: Context of the Organization**

- Internal & external issues (SWOT/PESTLE)
- Needs and expectations of interested parties
- ISMS scope and boundaries

Clause 5: Leadership

- Top management commitment
- Information security policy and roles
- Organizational roles, responsibilities & authorities

Clause 6: Planning

- Risk assessment & treatment methodology
- Risk register and Statement of Applicability (SoA)
- ISMS objectives and planning to achieve them
- Information security risk acceptance criteria

Module 3: Support, Operations & Documentation

Objective: Learn how to build and maintain ISMS operations and documentation. **Clause 7: Support**

- Resources, awareness, and competence

- Internal & external communication
- Documented information (version control, review)

Clause 8: Operation

- Operational planning and control
- Risk treatment plan execution
- Control implementation, monitoring, and evidence

Module 4: Monitoring, Auditing & Improvement

Objective: Cover auditing, non-conformities, and continual improvement processes. **Clause 9: Performance Evaluation**

- Internal audit program planning and execution
- Management review inputs & outputs
- ISMS KPIs & metrics

Clause 10: Improvement

- Nonconformities & corrective actions
- Continual improvement methodology
- Audit findings and corrective action lifecycle

Module 5: Annex A Controls Deep Dive (based on ISO 27002:2022)

Objective: Explore the 93 reorganized controls across 4 themes.
Organizational Controls (37 controls)

- Governance, roles & responsibilities
- Information classification
- Business continuity, suppliers, project security

People Controls (8 controls)

- Screening, training, disciplinary process
- Remote working and responsibility awareness

Physical Controls (14 controls)

- Entry controls, device security, asset handling

Technological Controls (34 controls)

- Access control, cryptography, logging, backup
- DLP, malware protection, secure development

Module 6: Implementation Roadmap & Certification Journey

Objective: Understand how to initiate and sustain an ISO 27001 program.
Topics:

- ISMS implementation lifecycle (PDCA model)
- Gap analysis & readiness checklist
- Documented artifacts and audit evidence
- Internal vs external audit process
- Certification steps and surveillance audits
- Auditor skills and responsibilities

Optional Add-ons / Labs :

- Risk register design & threat mapping (Excel)
- Sample SoA preparation
- ISO 27001 internal audit case study
- Incident log and CAPA tracker creation