TechEd Academy
Learn | Certify | Succeed

ACCREDITED CERTIFICATION

COURSE CURRICULUM

Information Security Management System

ISO/IEC 27001 Lead Auditor Training

Master the principles of information security, risk management, and audit processes. Accredited by TÜV SÜD.

Learn | Certify | Succeed

COURSE AGENDA

Table of Contents

Practical Approach

Exam Preparation

SECTION

COURSE CURRICULUM

Training Course Objectives & Structure

General Information

Overview of the course prerequisites, target audience, and administrative details ensuring a smooth learning experience.

Learning Objectives

Detailed breakdown of the knowledge and skills participants will acquire regarding ISMS implementation and auditing.

Educational Approach

Explanation of our teaching methodology, combining theoretical sessions with practical exercises and case studies.

Examination & Certification

Details on the exam format, passing criteria, and the prestigious TUV SUD accredited certification process.

Standards & Certification

Standards & Frameworks

Regulatory Context

02

- What is ISO? Understanding the International Organization for Standardization and its global role.
- The ISO/IEC 27000 Family Overview of the vocabulary (27000), requirements (27001), and guidelines (27002, etc.).
- Advantages of ISO/IEC 27001 Key business benefits including enhanced trust, regulatory compliance, and risk reduction.

Foundation of ISMS

Certification Process

Path to Compliance

03

- Certification Process From initial gap analysis to the final certification audit and issuance.
- Certification Scheme Understanding the 3-year certification cycle and surveillance requirements.
- Accreditation Bodies Role of bodies like UKAS, ANAB, etc. in authorizing certification bodies.
- Certification Bodies The organizations (e.g., TÜV SÜD) authorized to perform external audits.

04

SECTION

FUNDAMENTAL CONCEPTS

Information Security Principles

Assets & Information Security

Defining what constitutes an asset, understanding the nature of information, and the core definitions of information security.

The CIA Triad

The three essential pillars of information security: Confidentiality, Integrity, and Availability.

Risk, Threats & Vulnerabilities

Analyzing the relationship between vulnerabilities, threats, and their impact to determine information security risk.

Security Controls

Defining security control objectives and understanding the classification of controls (preventive, detective, corrective).

SECTION 05

COURSE CURRICULUM

Information Security Management System (ISMS)

Core Definitions

Understanding the foundational definitions of a management system and the specific scope of an ISMS within an organization.

Process Approach

Adopting the process approach for ISMS implementation, emphasizing the Plan-Do-Check-Act (PDCA) cycle for continuous improvement.

Clauses 4 to 10

Comprehensive overview of mandatory clauses: Context, Leadership, Planning, Support, Operation, Evaluation, and Improvement.

Annex A & SoA

Navigating the reference controls in Annex A and developing the crucial Statement of Applicability (SoA) for compliance.

SECTION 06

AUDIT PRINCIPLES, PREPARATION, AND INITIATION

Fundamental Audit Concepts & Principles

Standards & Definitions

Understanding ISO 19011 audit standards, the formal definition of an audit, and classifying audits into 1st, 2nd, and 3rd party types.

Roles & Objectives

Defining the audit criteria and objectives, while identifying the distinct roles of the client, auditor, and auditee.

Principles & Combined Audits

Exploring core principles like integrity and fair presentation, and the methodology for conducting combined management system audits.

Auditor Competence

Frameworks for determining necessary knowledge and skills, along with processes for the continuous evaluation of auditors.

SECTION

FUNDAMENTAL AUDIT CONCEPTS

Impact of Trends & Technology in Auditing

Big Data Analytics

Understanding the "Three V's" (Volume, Velocity, Variety) and leveraging big data analytics to enhance audit evidence coverage and reliability.

AI & Machine Learning

Exploring how artificial intelligence and machine learning algorithms are transforming automated control testing and anomaly detection.

Cloud Computing

Addressing the unique challenges and control objectives when auditing virtualized infrastructure and cloud-based services.

Auditing Outsourced Operations

Strategies for evaluating third-party risks and ensuring compliance in supply chains and outsourced business processes.

Audit Methodology

Evidence-based Auditing

08

Foundation of Conclusions

- Audit Evidence Records, statements of fact, or other information which are relevant to the audit criteria and verifiable.
- Types of Audit Evidence Includes physical examination, documentation review, interviews, and analytical procedures.
- Quality & Reliability Ensuring evidence is accurate, complete, relevant, and sufficient to support audit findings.

Objective & Verifiable

Risk-based Auditing

09

Strategic Focus

- Risk-based Approach Prioritizing audit activities and methods based on the significance of risks and their potential impact.
- Materiality & Planning Allocating time and resources to areas with the highest risk and materiality to the ISMS.
- Reasonable Assurance Providing a high level of confidence in conclusions, acknowledging that absolute assurance is rarely possible.

Targeted Effectiveness

Initiation & Stage 1 Audit

Initiation of Audit

Starting the Process

10

- Offer & Acceptance Defining the audit offer, assessing feasibility, and formally accepting the engagement.
- Team Selection Appointing the audit team leader and selecting competent team members.
- Engagement Establishing initial contact with the auditee to confirm arrangements.
- Audit Schedule Developing a timeline and schedule for audit activities.

Stage 1 Audit

Document Review

11

- Objectives Reviewing documentation and evaluating the client's readiness for Stage 2.
- Preparation Executing pre on-site activities and preparing necessary checklists.
- Conducting Activities Performing the on-site review to verify ISMS documentation status.
- Documenting Outputs Recording findings, areas of concern, and conclusions from the Stage 1 audit.

SECTION
ON-SITE AUDIT ACTIVITIES

Preparing for Stage 2 Audit

Setting the Audit Objectives

Defining clear goals and criteria for the Stage 2 audit to ensure full verification of the ISMS implementation and compliance.

Planning the Audit

Creating a detailed audit schedule including timing, locations, and specific departments or processes to be assessed during the visit.

Assigning Work to the Audit Team

Distributing roles and responsibilities among team members based on their specific competencies and expertise in relevant areas.

Preparing Audit Test Plans

Developing specific checklists and testing procedures to systematically verify the effectiveness of ISMS controls.

Preparing Documented Information

Ensuring all necessary documentation and records are available and organized for review to support audit evidence collection.

Stage 2 Audit & Communication

Stage 2 Audit Activities

13

Execution & Evidence Collection

- Opening Meeting Conducting the formal opening meeting to confirm the audit plan and introduce the team.
- Information Collection Gathering verifiable information through interviews, observation, and document review.
- Conducting Audit Tests Testing controls against audit criteria to verify effectiveness and compliance.
- Findings & Nonconformities Evaluating evidence to determine audit findings and drafting nonconformity reports (NCRs).
- Quality Review Reviewing audit work to ensure completeness and accuracy before closing.

Audit Communication

14

Interaction & Management

- Professional Behavior Maintaining professional conduct during on-site visits and respecting organizational culture.
- Effective Communication Ongoing communication within the audit team and regular updates to the auditee.
- Guides & Observers Managing the roles of guides and observers to ensure they do not influence the audit.
- Conflict Management Techniques for handling disagreements or difficult situations during the audit.
- Top Management Interaction Specific protocols for communicating audit progress and findings to senior leadership.

Procedures & Test Plans

Audit Procedures

15

Execution & Verification

Process Overview Comprehensive overview of evidence collection and analysis procedures throughout the audit lifecycle.

Collection Methods Gathering objective evidence via interviews, direct observation of processes, and review of documented information.

Verification Techniques Validating findings through analysis, systematic sampling methods, and technical verification of controls.

Evidence-Based Approach

Creating Audit Test Plans

16

Strategy & Guidance

Audit Test Plans Developing effective test plans with practical examples to guide specific audit activities.

ISMS Guidance Specific guidelines for auditing an Information Security Management System effectively.

Evaluation & Corroboration Techniques for corroborating evidence and evaluating findings against audit criteria.

Virtual Auditing Special considerations and methods for auditing virtual activities and remote locations.

AUDIT LIFECYCLE PHASE 3 & 4

Closing, Reporting & Follow-up

Detailed procedures for finalizing the audit and managing post-audit activities

Section 17

Drafting Findings & NCRs

- Categorizing audit findings
- Documenting nonconformities accurately
- Drafting the formal NCR
- Principle: "Benefit of the doubt"

Section 18

Documentation & Review

- Managing work documents
- Conducting quality reviews
- Ensuring traceablity of evidence

Section 19

Closing of the Audit

- Determining audit conclusions
- Conducting the closing meeting
- Preparing & distributing report
- Making the certification decision

Section 20

Evaluation of Action Plans

- Submission by the auditee
- Content requirements for plans
- Auditor's evaluation process

Section 21

Beyond the Initial Audit

- Audit follow-up activities
- Surveillance audits (Years 1 & 2)
- Recertification audit (Year 3)
- Proper use of trademarks

FINAL PHASE AUDIT MANAGEMENT & CERTIFICATION

Program Management & Exam Prep

Managing internal audit programs, practical application, and certification readiness

Section 22

Audit Program Mgmt.

- Role of internal audit function
- Defining audit services & activities
- Managing program resources
- Maintaining audit program records

Section 23

Monitoring & Improvement

- Follow-up on nonconformities
- Monitoring program performance
- Reviewing & improving the program

ISO 27001 Applied

- New 93 Controls to Evidence Mapping
- Practical evidence collection guide
- 3 real-world audit scenarios
- Case study analysis

Course Review & Mock Exam

- Comprehensive course revision session
- Open mic session for doubts & Q&A
- Full-length mock examination

Certification Success

- Detailed discussion on exam questions
- Analysis of answer strategies
- Overview of different exam formats

CONTACT US

Thank You !

Contact us if you have any questions about the training program.

+91 88302 38589

www.techedacademy.com

support@techedacademy.com