TRANCHULAS

ISO 27001 Implementation Training Course

Master ISO 27001: Expert-Level ISMS Implementation & Security Excellence

Introduction

This three-day hands-on, intensive course provides comprehensive training in implementing and managing ISO 27001 Information Security Management Systems (ISMS). Through practical workshops and real-world case studies, participants gain the expertise needed to design, implement, and maintain robust information security management systems that protect critical business assets and ensure compliance with international standards.

Accreditations

Tranchulas is a CREST Cyber Training Provider, validating the excellence and credibility of our training offerings.

Course Objectives

By the end of this course, participants will be able to:

1. Understand the ISO 27001 standard and its requirements for implementing an effective Information Security Management System (ISMS).
2. Conduct comprehensive risk assessments using ISO 27005 methodologies, including asset identification, threat analysis, and vulnerability assessment.
3. Develop and implement risk treatment plans that align security controls with business objectives and regulatory requirements.
4. Implement and manage all 93 ISO 27001 Annex A controls across organizational, people, physical, and technological domains.
5. Create comprehensive ISMS documentation including policies, procedures, and records that meet certification requirements.
6. Plan and conduct internal audits to assess ISMS effectiveness and identify areas for improvement.
7. Prepare for and manage external certification audits, including Stage 1 and Stage 2 assessments.

Course Outline

Day 1: ISMS Foundations & Strategic Planning

Module 1: Introduction to ISO 27001 & ISMS

- Understanding ISO 27001 Standard
- Information Security Management System (ISMS) Overview
- ISO 27001:2022 Structure and Requirements
- Benefits of ISO 27001 Certification
- ISMS Lifecycle and Implementation Roadmap

Module 2: Context of the Organization

- Understanding Organizational Context
- Identifying Internal and External Issues
- Stakeholder Requirements and Expectations
- Defining ISMS Scope and Boundaries
- Leadership and Commitment Requirements

Module 3: Information Security Policy & Governance

- Developing Information Security Policy
- Establishing Governance Framework
- Roles and Responsibilities Definition
- Management Commitment and Support
- Communication and Awareness Strategies

Module 4: Risk Assessment Fundamentals

- Introduction to Risk Management (ISO 27005)
- Asset Identification and Classification
- Threat and Vulnerability Analysis
- Risk Assessment Methodologies
- Risk Criteria and Acceptance Levels
- Exercise: Conduct asset inventory and initial risk identification

Day 2: Risk Treatment & Control Implementation

Module 5: Risk Treatment Planning

- Risk Treatment Options (Modify, Retain, Avoid, Share)
- Selecting Appropriate Controls
- Statement of Applicability (SoA) Development
- Risk Treatment Plan Creation
- Resource Allocation and Prioritization
- Exercise: Develop risk treatment strategies for identified risks

Module 6: ISO 27001 Annex A Controls - Part 1 (Organizational Controls)

- Organizational Controls
- People Controls
- Physical Controls
- Control Implementation Strategies
- Policy and Procedure Documentation
- Exercise: Map organizational controls to business requirements

Module 7: ISO 27001 Annex A Controls - Part 2 (Technical Controls)

- Technological Controls
- Access Control Implementation
- Cryptography and Key Management
- Network Security Controls
- Secure Development Practices
- Cloud Security Considerations

Module 8: Documentation & Record Management

- ISMS Documentation Requirements
- Policy, Procedure, and Work Instruction Development
- Record Keeping and Evidence Management
- Document Control Processes
- Version Control and Change Management
- Exercise: Create sample ISMS documentation package

Day 3: Audit, Monitoring & Continuous Improvement

Module 9: Performance Monitoring & Measurement

- Establishing Performance Metrics
- Monitoring and Measurement Processes
- Key Performance Indicators (KPIs)
- Security Metrics and Reporting
- Management Review Requirements

Module 10: Internal Audit Program

- Internal Audit Planning and Preparation
- Audit Methodologies and Techniques
- Conducting Effective Audits
- Non-Conformity Identification
- Audit Reporting and Follow-up
- Exercise: Conduct mock internal audit scenarios

Module 11: Incident Management & Business Continuity

- Information Security Incident Management
- Incident Response Planning
- Business Continuity and Disaster Recovery
- Testing and Exercising Plans
- Lessons Learned and Improvement

Module 12: Certification Process & Continuous Improvement

- Certification Audit Preparation
- Stage 1 and Stage 2 Audit Process
- Managing External Auditors
- Non-Conformity Management and Corrective Actions
- Continual Improvement Cycle (Plan-Do-Check-Act)
- Surveillance and Re-certification Audits
- Exercise: Prepare for certification audit with mock scenarios

Module 13: Advanced Topics & Best Practices

- Integration with Other Management Systems
- Emerging Threats and Technologies
- AI and Cloud Security in ISMS Context
- Supply Chain Security Management
- Building Security Culture
- Final Q&A and Course Review