deerwalk training center

DTI- ISO -101

ISO 27001:2022 Training Align with Course Content

deerwalktrainingcenter.com

Program Information

Nature of the Course
Theory + Practical

Total Hours per Day
8 hours

Course Duration
15 Days

Course Summary

The ISO 27001:2022 course offers a comprehensive guide to understanding and implementing an Information Security Management System (ISMS) in organizations. Participants will learn the essential elements of the standard, including risk management processes, security controls, and the framework needed to protect sensitive information. This course also highlights the key updates in the 2022 version, focusing on new requirements, changes in risk-based thinking, and emerging trends in information security.
By the end of the course, participants will have the knowledge to establish, implement, maintain, and continually improve an ISMS in line with ISO 27001:2022 standards. The training prepares attendees for the certification process, equipping them with the skills to lead internal audits, manage compliance, and address information security challenges effectively.

Completion Criteria

After fulfilling all of the following criteria, the student will be deemed tohave finished the Module:

- Has attended 90% of all classes held.

Required Textbooks

- No textbooks are required

Prerequisites

- Participants should have a basic understanding of information security concepts and principles.
- It is recommended to have prior knowledge of risk management, organizational processes, and the importance of information security standards.
- While no formal certifications are required, a foundational understanding of ISMS or ISO 27001 (previous versions) would be beneficial.

Course Details

Day 1: Course Introduction and Overview

General Information
- Introduction to the course
- Importance of ISO 27001:2022

Learning Objectives
- Define what participants will learn
- Expected outcomes

Educational Approach
- Interactive sessions
- Practical exercises and case studies

Examination and Certification
- Examination format
- Certification process

What is ISO?

The ISO/ IEC 27000 Family of Standards:
- Overview of the standards
- Scope and applicability

Advantages of ISO/ IEC 27001:
- Benefits for organizations
- Case studies of successful implementations

Day 2: Certification Process

Certification Process
- Introduction to the course
- Importance of ISO 27001:2022

Certification Scheme:
- Detailed look at certification requirements

Accreditation Bodies
- Roles and responsibilities

Certification Bodies:

- Selection criteria
- How to engage with them

Interactive sessions

- Practical exercises and case studies

Day 3: Fundamentals Concepts and Principles of Information Security

Information and Asset:

- Definition and examples

Information Security:

- Key concepts and definitions

Confidentiality, Integrity and Availability (CIA):

- Core principles

Vulnerability, Threat, and Impact:

- Definitions and relationships

Information Security Risk:

- Key concepts and definitions

Security Controls and Control Objectives:

- Purpose and types

Classification of Security Controls:

- Preventive, detective, corrective

Interactive sessions

Practical exercises and case studies

Day 4: Information Security Management System (ISMS)

Definition of a Management System:

- Key components

Definitions of ISMS:
- Structure and purpose

Process Approach:
- Importance of ISMS

ISMS Implementation:
- Steps and best practices

Overview of Clauses 4 to 10:
- Key requirements

Overview of Annex A:
- Controls and their objectives

Statement of Applicability:
- How to create and use it

Interactive sessions

Practical exercises and case studies

Day 5: Fundamental Audit Concepts and Principles

Audit Standards:
- Overview and importanc

What is an Audit?
- Definition and purpose

Types of Audits:
- Roles and responsibilities

Audit Objectives and Criteria:
- Setting and evaluating objectives

Combined Audit:
- Benefits and challenges

Principle of Auditing:
- Key principles

Competence and Evaluation of Auditors:
- Skills and assessment

Interactive sessions

Practical exercises and case studies

Day 6: Impact of Trends and Technology in Auditing

Big Data:
- Definition and significance

The Three V of Big Data:
- Volume, variety, velocity

Use of Big Data in Audits:
- Applications and examples

Artificial Intelligence:
- Overview and impact on audits

Machine Learning:
- Applications in auditing

Cloud Computing:
- Auditing cloud environments

Auditing Outsourced Operations:
- Challenges and solutions

Interactive sessions

Practical exercises and case studies

Day 7: Evidence- Based Auditing

Audit Evidence:
- Definition and importance

Types of Audit Evidence:
- Documentary, testimonial, analytical

Quality and Reliability of Audit Evidence:
- Criteria for evaluation

Interactive sessions

Practical exercises and case studies

Day 8: Risk-Based Auditing

Audit Approach Based on Risk:

- Principles and Methods

Materiality and Audit Planning:

- Determining materiality

Reasonable Assurance:

- Concept and application

Interactive sessions

Practical exercises and case studies

Day 9: Initiation of the Audit Process

The Audit Offer:

- Developing and presenting the offer

The Audit Team Leader:

- Roles and responsibilities

The Audit Team:

- Selection and composition

Audit Feasibility:

- Assessing feasibility

Adult Acceptance:

- Formal acceptance process

Establishing Contact with the Auditee:

- Communication strategies

The Audit Schedule:

- Planning and scheduling

Interactive sessions

Practical exercises and case studies

Day 10: Stage 1 Audit

Objectives of the stage 1 Audit:
- Goals and scope

Pre-On Site Activities:
- Preparation and planning

Preparing for On-Site Activities:
- Checklist and resources

Conducting On- Site Activities
- Steps and best practices

Documenting the Outputs of Stage 1 Audit:
- Report writing

On site Audit Activities:

Interactive sessions

Practical exercises and case studies

Day 11: Preparing for Stage 2 Audit:

Setting the Audit Objectives:
- Defining clear objectives

Planning the Audit:
- Detailed planning

Assigning Work to the Audit Team:
- Roles and responsibilities

Preparing Audit Test Plans:
- Developing test plans

Preparing Documented Information for the Audit:
- Documentation review

Interactive sessions

Practical exercises and case studies

Day 12: Stage 2 Audit

Conducting the Opening Meeting:
- Agenda and key points

Collecting Information:
- Methods and tools

Conducting Audit Tests:
- Execution and documentation

Determining Audit Findings and Non-Conformity Reports:
- Identifying and reporting issues

Performing Quality Review:
- Ensuring accuracy and completeness

Interactive sessions

Practical exercises and case studies

Day 13: Communication During the Audit

Behavior During On-Site Visits:
- Professional conduct

Communication During the Audit:
- Effective communication strategies

Audit Team Meetings:
- Coordination and updates

Guides and Observes:
- Roles and interaction

Conflict Management:
- Handling disagreements

Cultural Aspects:
- Awareness and sensitivity

Communication with Top Management:
- Strategies for effective engagement

Interactive sessions

Practical exercises and case studies

Day 14: Audit Procedures and Test Plans

Overview of the Audit Process:
- Step-by-step guide

Evidence Collection and Analysis Procedures:
- Methods and best practices

Interview Techniques:
- Conducting effective interviews

Documented Information Review:
- Evaluating documentation

Observation and Analysis:
- Practical exercises

Sampling and Technical Verification:
- Methods and examples

Creating Audit Test Plans:
- Developing and refining test plans

Interactive sessions

Practical exercises and case studies

Day 15: Conducting the Audit and Practical Approaches

Drafting Audit Findings and Non-Conformity Reports:
- Writing and documenting findings

Audit Documentation and Quality Review:
- Ensuring thorough documentation

Closing of the Audit:
- Determining and discussing conclusions

Evaluation of Action Plans by the Auditor:
- Reviewing and evaluating action plans

Beyond the Initial Audit:

- Follow up and surveillance activities

ISO 27001 Practical Approaches:

- Controls to evidence mapping
- Case studies and scenarios

Examination and Certification

Examination:

- Conduct exam questions practice sessions

Labs

Lab assignments will focus on the practice and mastery of contents covered in the lectures, and introduce critical and fundamental problem solving techniques to the students.

Learning Outcomes

- Understand ISO 27001:2022 principles and its role in information security.
- Gain knowledge of the ISO/IEC 27000 family, scope, and applicability.
- Learn the steps, timeline, and requirements for ISO 27001 certification.
- Understand key information security principles like CIA and risk management.
- Learn to implement an ISMS, including clauses 4 to 10 and Annex A.
- Grasp audit concepts, principles, objectives, and auditor competencies.
- Apply risk-based auditing methods and ensure reasonable assurance.
- Understand the impact of emerging technologies on auditing (e.g., Big Data, AI).
- Learn to collect, analyze, and evaluate audit evidence.
- Develop effective communication strategies during audits and conflict management.
- Master creating audit test plans, conducting audits, and ensuring compliance.
- Understand the preparation, objectives, and execution of Stage 1 and Stage 2 audits.
- Gain skills in drafting audit findings, writing reports, and audit closures.
- Learn follow-up activities, action plan evaluations, and surveillance post-audit.
- Prepare for the final examination and certification through practice sessions.

deerwalk
training center

Sifal, Kathmandu, Nepal
Phone: +977 - 01 - 5913021 | 4567153
Mobile: +977 - 9765355167 | 9860422021
Email: training@deerwalkcompware.com
Website: deerwalktrainingcenter.com