ISO 27001:2022 AWARENESS TRAINING

Certificate of Completion: ISO 27001:2022 Awareness Training

Course Code: M044/25

Duration: 8 Hours

Delivery Format: Hybrid

Target Audience:

This course is intended for company personnel who are considering the development and implementation of an Information Security Management System that meeting ISO 27001:2022 to achieve third party certification and is particularly relevant to the ISMS steering group representative.

Program Outcomes:

Upon completion of this program, participants will be able to:

- Understand information and the various risks to which it is subjected.
- Learn techniques that cover the requirements of ISO 27001:2022.

Detailed Syllabus

Module 1: Background to Changes from Old Version to New Version

Outcome: Participants will understand the historical context and key drivers behind the changes leading to the ISO 27001:2022 standard.

Topics:

- ISO 27001 revisions since beginning

Activities:

- Presentation on the history of ISO 27001 and its revisions.
- Comparison of key differences between the old and new versions.

Assessments:

- Short quiz on the timeline and key drivers of ISO 27001 revisions

Module 2: Context of the Organization

Outcome: Participants will be able to define the internal and external context of an organization, identify relevant interested parties and their requirements, and establish the scope of an Information Security Management System (ISMS). They will also understand the basics of an IS Risk Register and Opportunity Register.

Topics:

- Understanding the organization and its context
- Understanding the needs and expectations of interested parties
- Determining the scope of the ISMS
- Identification of internal and external issues and identifying interested parties and their requirements and development of IS Risk Register and Opportunity Register.

Activities:

- Interactive exercises on analyzing organizational context (SWOT, PESTLE).
- Group work on identifying interested parties and their relevant requirements.

Assessments:

- Short case study: Defining the context and interested parties for a hypothetical organization

Module 3: Leadership

Outcome: Participants will understand the leadership requirements of ISO 27001:2022, including the importance of commitment, establishing a security policy, and defining organizational roles and responsibilities.

Topics:

- Leadership and commitment
- Security policy
- Organization roles, responsibilities, and authorities

Activities:

- Discussion on the role of top management in information security.
- Analysis of the key elements of an effective security policy.

Assessments:

- Identifying the key responsibilities of leadership in ISO 27001:2022

Module 4: Planning

Outcome: Participants will be able to identify and plan actions to address information security risks and opportunities, set security objectives, and plan for changes within the ISMS.

Topics:

- Actions to address risks and opportunities
- Examples of risks
- Effective risk management
- Actions to address risks and opportunities
- Security objectives and planning to achieve them
- Planning of changes

Activities:

- Introduction to risk assessment and treatment methodologies.
- Examples of common information security risks and opportunities.

Assessments:

- Developing a basic risk treatment plan for an identified risk

Module 5: Support

Outcome: Participants will understand the support requirements of ISO 27001:2022, including the need for adequate resources, competence, awareness, communication, and documented information.

Topics:

- Resources
- People
- Infrastructure
- Competence

- Awareness
- Communication
- Documented information

Activities:

- Discussion on the necessary resources for an effective ISMS.
- Importance of ensuring competence and providing awareness training.

Assessments:

- Identifying the key elements of support required by ISO 27001:2022

Module 6: Operation

Outcome: Participants will understand the operational planning and control requirements of ISO 27001:2022, including the implementation of operational risk management processes.

Topics:

- Operational planning and control
- Operational risk management

Activities:

- Guidance on establishing and maintaining operational controls.
- Detailed discussion on the operational risk management process.

Assessments:

- Describing the key steps in operational risk management

Module 7: Performance Evaluation

Outcome: Participants will understand the requirements for monitoring, measuring, analyzing, and evaluating ISMS performance, including conducting internal audits and management reviews.

Topics:

- Monitoring, measurement, analysis and evaluation
- Analysis and evaluation
- Internal audit
- management review

Activities:

- Overview of the internal audit process and its objectives.
- Explanation of the purpose and requirements of management reviews.

Assessments:

- Identifying the objectives of an internal audit

Module 8: Improvement

Outcome: Participants will understand the requirements for addressing nonconformities, taking corrective actions, and implementing continual improvement within the ISMS.

Topics:

- General
- Nonconformity and corrective action
- Continual improvement

Activities:

- Discussion on the process for identifying and managing nonconformities.
- Guidance on implementing effective corrective actions.

Assessments:

- Describing the steps involved in addressing a nonconformity