ISO 27001:2016 Information Security Management System
(ISMS) Training

Phase #1 (2 Days)

Principles of a Quality Management System - ISO27001

- What is ISO, and its origins.
- What ISO 27000 standards are about.
- Why ISO? How to get benefits from ISO27001. ISO27001 explanation and requirements.

Detailed review of the ISO standard. (Clause by clause review discussion/answer questions.)

- Introduction
- Scope
- Normative references
- Terms and definitions
- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

Annex A Reference control objectives and controls touching on the following topics

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development & maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of BCM
- Compliance

PDCA (Plan-Do-Check-Act). How to properly implement ISO using PDCA model

- **Plan**: Establish the objectives and processes necessary to deliver results in accordance with customer requirements and the organizations policies
- **Do**: Implement the processes
- **Check**: Monitor and measure processes and product against policies, objectives and requirements for the product and report the results
- **Act:** Take actions to continually improve process performance

Phase #2 (6 Days)
ISO27001 Quality System Development

Having learned about ISO, we will train towards the Development of an ISO compliant system by addressing specific items needed for registration and more importantly by the company for success. The items are, paced over time.

Discuss the components of ISO27001 and how to develop Documented Information that meets company needs, customer needs and ISO27001.

Documentation Required per ISO27001 as applicable to the organization Discuss the following information to enable the creation of an ISMS system.

The following mandatory documentation (or rather "documented information") is explicitly required for certification and thus will be discussed:

- ISMS scope (as per clause 4.3)
- Information security policy (clause 5.2)
- Information security risk assessment *process* (clause 6.1.2)
- Information security risk treatment *process* (clause 6.1.3)
- Information security objectives (clause 6.2)
- Evidence of competence of people working in information security (clause 7.2)
- Other ISMS documents deemed necessary by the organization (clause 7.5.1b)
- Operational planning and control documents (clause 8.1)
- The *results* of the risk assessments (clause 8.2)
- The *decisions* regarding risk treatment (clause 8.3)
- Evidence of the monitoring and measurement of information security (clause 9.1)
- The ISMS internal audit program and the results of audits conducted (clause 9.2)
- Evidence of top management reviews of the ISMS (clause 9.3)
- Evidence of nonconformities identified and corrective actions (clause 10.1)
- Various others per Annex A, which is normative
    - including the rules for acceptable use of assets, access control policy
    - operating procedures
    - confidentiality or non-disclosure agreements

- secure system engineering principles,
- information security policy for supplier relationships
- information security incident response procedures
- relevant laws
- regulations and contractual obligations plus the associated compliance procedures and information security continuity procedures.

Learn how to create other documents needed that will benefit the company

Work on responsibilities/authorities and methods for satisfying the standard. i.e., job descriptions, final org charts, etc.

Homework assignments

Homework between sessions will be assigned. The homework will be reviewed at the following session prior to starting a new session.

Phase #3 (4 Days)
ISO27001 Implementation of ISMS Requirements

Learn to properly implement all phase 2 trained to per Phase 2 over time in segments to assure success. Learn how to create the

- ISMS scope
- Statement of Applicability (SoA)
- Learn how to perform RISK Analysis, using the SoA and ensuring that all parts of the organization benefit by addressing their information security risks in an appropriate and systematically-managed manner.
- Prepare / Conduct a management review using the established procedure(s)
- Develop an agenda template and discuss who should participate. What topics should be included for an effective management review will be covered such as
- Learn how to use the information by top management to assure
- Opportunities for improvement
- Any need for changes to the management system
- Resource needs

Training will address how to facilitate a management review meeting.

Training on the use of suitable methods for monitoring and, where applicable, measurement of the management system processes.

How to determine, collect and analyze appropriate data to demonstrate the suitability and effectiveness of the management system and to evaluate where continual improvement of the effectiveness of the management system can be made.

Training on how to include data generated as a result of monitoring and measurement and from other relevant sources.

Learn methods to continually improve the effectiveness of the management system through the use of:

- the policy
- objectives
- audit results
- analysis of data
- corrective and preventive actions
- management review and other information available to the organization

Focus of the training will be the

- Implementation Roadmap
- Risk Management
- Security profile and action plan on how to achieve it
- Implementing controls based on risk analysis
- Operating the ISMS
- Monitoring and measurement of the ISMS

Phase #4 (3 Days)
ISO27001 Internal Auditor training

Conduct Auditor Training

The basis for this training is to perform ISO 19011 auditor training to help trainees develop their own internal capability to perform Internal Quality Audits as required per ISO27001 The training will consist of:

- ISO27001 Overview (Summary of key requirements that need to be audited)
- ISO19011:2002 Guidelines for Quality and/or environmental management systems auditing

Preparing for the audit - Planning, scheduling, audit team, preparation, checklists, etc.

The audit – Execution, Checklists and Audit techniques

After the audit – Closing meeting and reporting (Including CAPA's)

Additional learning will result in;

- Understanding of the Process Approach
- Identify the requirements of an auditor
- Form an audit team
- Plan, prepare and execute an audit
- Classify, record, and resolve nonconformities
- How to implement preventative measures to avoid future nonconformities

Trainees will conduct an Internal Audit using the methods learned under supervision for hands on training.

- Discuss what you should expect at registration. Discuss the various outcomes of an audit.
- Policy
- Goals and objectives
- Review existence of minimum requirements for audit readiness by registrar.

Phase 5 (3 Day)
ISO27001 ISMS Training for All employees
ISO27001 Overview

Inform/train remaining employees on what the management system is composed of, where the system documentation is located, how to get access to the documentation and how to use them for maximized benefit to the organization.

Learn methods for improving the system.

Learn how to be audited in an effective way by customers, registration bodies and internal auditors.

The training will address how to Apply suitable methods for monitoring and, where applicable, measurement of the quality management system processes.

How to determine, collect and analyze appropriate data to demonstrate the suitability and effectiveness of the quality management system and to evaluate where continual improvement of the effectiveness of the quality management system can be made.

How to include data generated as a result of monitoring and measurement and from other relevant sources.

How to analyze data / information

Expose the company to the created items in Phase 2 as implemented in phase 3

During the ISMS creation and implementation, the following documents may be written as needed and thus exposing those that need to know will be part of this session. The items that may be covered are:

- **Procedure for Document and Record Control** – procedure prescribing basic rules for writing, approving, distributing and updating documents and records
- **Procedure for Identification of Requirements** – procedure for identification of statutory, regulatory, contractual and other obligations
- **Scope of the Information Security Management System** – a document precisely defining assets, locations, technology, etc. that are part of the scope
- **Information Security Policy** – this is a key document used by management to control information security management
- **Risk Assessment and Risk Treatment Methodology** – describes the methodology for managing information risks
- **Risk Assessment Table** – the table is the result of assessment of asset values, threats and vulnerabilities
- **Risk Treatment Table** – a table in which appropriate security controls are selected for each unacceptable risk
- **Risk Assessment and Risk Treatment Report** – a document containing all key documents made in the process of risk assessment and risk treatment
- **Statement of Applicability** – a document that determines the objectives and applicability of each control according to Annex A of the ISO 27001 standard
- **Procedure for Internal Audit** – defines how auditors are selected, how audit programs are written, how audits are conducted and how audit results are reported
- **Procedure for Corrective Action** – describes the process of implementation for corrective and preventive actions
- **Form for Management Review Minutes** – a form used to create minutes from the management meeting held to review ISMS adequacy
- **Risk Treatment Plan** – an implementation document specifying controls to be implemented, who is responsible for implementation, deadlines and resources

Additional items may be:

- **Business Impact Analysis (BIA) questionnaires** – analysis of qualitative and quantitative impacts on business, of necessary resources, etc.
- **Business Continuity Plan** – a detailed description of how to respond to disasters or other business disruptions, and how to recover all critical activities
- **Post-incident Review Form** – a form used for reviewing effectiveness of plans after an incident