

## ISO 27001 Implementation Course – 3 Days

### INTRODUCTION and LEARNING OBJECTIVE

Information is a valuable asset for an organization. Securing Information of all types throughout its lifecycle is a multifold challenge. Technology alone is not sufficient to implement robust Information Security Program for an organization. Technology has to be backed by People and Processes and driven by management framework to reap the benefits of Information Security initiatives.

BS ISO/IEC 27001:2005, the standard for Information Security Management System (ISMS), fits the bill. More and more organizations of diverse size and business sectors are looking at this standard as the best practice and over 4000 of them are certified already.

The challenge is to find sound professional(s) who can drive Information Security Program with a balanced approach. Here, we present a power packed course that takes you through the introduction to information security concepts to the nitty-gritty's of implementation of ISO 27001.

At the end of this course you would be able to

- a. Understand Information Security Concepts
- b. Understand the challenges in handling Information security roles
- c. Create a business case for Information Security initiatives
- d. Understand requirements of ISO 27001
- e. Define Scope for ISO 27001
- f. Conduct Risk Assessment
- g. Prepare Risk Treatment plans
- h. Prepare Statement of Applicability
- i. Develop ISMS Manual
- j. Develop strategy and plans for ISMS roll out
- k. Monitor and review progress of ISMS activities
- l. Drive the team for achieving ISO 27001 certification

At the end of this course, the participant will be equipped to play a role and make significant contribution as

- a. Chief Information Security Manager
- b. Information Security Manager
- c. Information Security Analyst
- d. Information Security Consultant

## ISO 27001 Implementation Course – 3 Days

### PARTICIPANT PROFILE

You could be an individual who has basic knowledge of IT and business processes.

### DIFFERENTIATORS

The course is

- a. Comprehensive (Covers basics to advanced knowledge)
- b. Practical (Equips you with workable solutions)
- c. Activity oriented (Group case studies and individual presentations)
- d. Delivered by experienced professionals with great passion for training
- e. Collaborative learning approach (Making you participate and learn)

### AGENDA

Sr. #	Topics	Duration
<b>Day – I</b>		
1.	Information Security Concepts	1 hour
2.	Preparing Business Case for ISMS Implementation	1 hour
3.	Introduction to ISO 27000 family	1 hour
4.	Awareness on ISO 27001 (Clauses and Annexure – A)	4 hours
<b>Day – II</b>		
1.	Establish ISMS - Determination of Scope and Develop ISMS Policy	2 hours
2.	Establish ISMS – Define risk assessment approach	3 hours
3.	Establish ISMS – Identify, Analyze and evaluate risks	
4.	Establish ISMS – Identify and evaluate options for risk treatment	1 hour
5.	Establish ISMS - Selection of Controls and preparing SOA	1 hour
<b>Day – III</b>		
1.	Establish ISMS – Documentation	2 hours
2.	Implement and Operate ISMS	
3.	Monitor and Review ISMS	2 hours

### ISO 27001 Implementation Course – 3 Days

4.	Maintain and Improve ISMS	
5.	Certification Audits	1 hour
6.	Review and Exam	1 hour

## DAY – I

### Information Security Concepts

- ⇒ Fundamentals information security and its principles
- ⇒ Business Requirements of information security
- ⇒ Compliance issues
- ⇒ Types of laws, regulations and crimes
- ⇒ Consequences
- ⇒ Information Security best practices

### Preparing Business Case for ISMS Implementation

- ⇒ Rationale
- ⇒ Proposed Solution – ISO 27001
- ⇒ Benefits of ISO 27001
- ⇒ Proposed Approach and Methodology
- ⇒ Project Risks

### Introduction to ISO 27000 Family

- ⇒ History of ISO 27000 family
- ⇒ Features of the standard
- ⇒ PDCA Process approach
- ⇒ Structure of standard

### Awareness on ISO 27001

- ⇒ 1 Scope
- ⇒ 2 Normative References
- ⇒ 3 Terms and Definitions
- ⇒ 4 Information Security Management System
- ⇒ 5 Management Responsibility
- ⇒ 6 Internal ISMS Audits
- ⇒ 7 Management Review of the ISMS
- ⇒ 8 ISMS Improvement
- ⇒ Annexure – A Control Objectives and Controls

## ISO 27001 Implementation Course – 3 Days

### DAY – II

#### **Establish ISMS – Determination of Scope and Develop ISMS Policy**

- ⇒ Understand the requirement of the standard
- ⇒ Determine the details to define the scope of ISMS
- ⇒ Identify Management's intent to implement ISMS
- ⇒ Determine various roles and responsibilities
- ⇒ Assignment – (Writing the scope statement, ISMS Policy)

#### **Establish ISMS – Define Risk Assessment Approach**

- ⇒ Risk Assessment Concepts
- ⇒ Understand Risk Analysis techniques (Qualitative v/s Quantitative)
- ⇒ Define Risk Assessment approach

#### **Establish ISMS – Identify, Analyze and Evaluate Risks**

- ⇒ Identification of Assets
- ⇒ Classification and Valuation of Assets
- ⇒ Identify threats and vulnerabilities
- ⇒ Determine the likelihood
- ⇒ Estimate risk levels and impacts
- ⇒ Establish a criteria for risk acceptance
- ⇒ Assignment – (Conduct RA)

#### **Establish ISMS – Identify and Evaluate options for Risk Treatment**

- ⇒ Develop Risk Treatment Plans
- ⇒ Selecting appropriate Control Objectives and Controls
- ⇒ Prepare Statement of Applicability
- ⇒ Assignment – (Prepare RTP)

## ISO 27001 Implementation Course – 3 Days

### DAY – III

#### **Establish ISMS - Documentation**

- ⇒ Understand ISMS Documentation Requirements
- ⇒ ISMS Mandatory Documents, Policy Framework, Procedures
- ⇒ Assignment – (Develop a sample Policy)

#### **Implement and Operate ISMS**

- ⇒ ISMS Roll out plans, resource management
- ⇒ Strategy and Plans to spread ISMS awareness across the user base
- ⇒ Security incident response

#### **Monitor and review ISMS**

- ⇒ Internal audit charter
- ⇒ Internal audit policy
- ⇒ Internal Audit program
- ⇒ Management review

#### **Maintain and Improve ISMS**

- ⇒ Corrective Actions
- ⇒ Preventive Actions
- ⇒ Continual Improvement

#### **Certification Audit**

- ⇒ Accreditation Schemes
- ⇒ Certification Body
- ⇒ Certification process for ISO 27001
- ⇒ Integrated Management Framework
- ⇒ Other important ISO standards

#### **Exam**

- ⇒ 40 Multiple choice Questions
- ⇒ Duration : 1 Hour
- ⇒ Passing percentage: 75
- ⇒ Unsuccessful candidate gets a participation certificate
- ⇒ Successful candidate gets a completion certificate
- ⇒ Unsuccessful candidate can re-appear exam

--- End of Document ---