

Stages for Deployment of ISO 27001:2005

Information Technology -Code of Practice for Information Security Management)

1. Stage 1

- a) GAP Analysis
- b) Project Initiation & Preparing Project Scope Document and Sign-off
- c) Awareness Training.
- d) Scope of ISMS (Information Security Management System)
- e) Forming Information Security Steering Committee and appointment of Information Systems Security officer

2. Stage 2

- a) Risk Assessment.
 - ❖ Enumerating the business processes
 - ❖ Enumerating Information Assets within the scope and in the defined business processes
 - ❖ Asset Valuation
 - ❖ Threat Assessment
 - ❖ Process Vulnerability Assessment
 - ❖ Technical Vulnerability Assessment
 - ❖ Penetration Testing
 - ❖ Likelihood determination
 - ❖ Risk Determination
 - ❖ Risk Assessment Documentation
- b) Documentation. (Assistance in preparation including providing of requisite samples / templates) of the following
 - ❖ ISMS Policy
 - Designing detailed Information Security Policies
 - ❖ Risk Treatment Plan, Statement of Applicability
 - Identifying the Risks which are acceptable/ transferable and avoidable
 - Acceptance from the management where a business has decided to accept risks
 - Selection of controls for Risk reduction
 - Identification of applicable ISO 27001
 - Preparing Selection of control objectives, controls and existing/planned controls
 - Management approval for residual risks
 - Preparation of Risk Treatment Plan
 - Preparation of Statement of Applicability
 - ❖ Design Procedures needed for implementation of ISMS
 - ❖ Disaster Recovery and Business Continuity Plan
 - Preparing the Policy
 - Preparing a Plan
 - Preparing test Plan
 - Preparing Call tree
 - ❖ Designing Formats

3. Stage 3

- a) Internal Auditors Course for designated personnel.
- b) Implementation of the designed system.

4. Stage 4

- a) Audit Charter, Preparing the Audit templates & yearly Audit Plan
 - ❖ Internal ISMS Audit
 - ❖ Corrective Action and Information Security Steering Committee Review Meeting.

5. Stage 5 Certification Audit (Pre & Final Audit by Certification Body)