

www.uaeiso.com

ISO 27001

Information Security Management Systems Implementation Road Map



ISO
27001:2013
INFORMATION SECURITY

10 Step Approach to ISO 27001 Certification

- **Awareness Training**
- **Information Security Policy and Objectives Finalization**
- **Gap Analysis / Risk Assessment**
- **Documentation / Process Design**
- **Documentation / Process Implementation**
- **Internal Audit**
- **Management Review Meeting**
- **Pre-assessment Audit**
- **Corrective – Preventive Actions**
- **Final Certification Audit & Award of Certification**



Step 1: Awareness Training



Deliverables:-

Organization wide awareness about Information Security Management System and ISO 27001.

- Separate Training Sessions for Top Management, Middle Management and Junior level Management.
- Creates a motivating environment throughout the organization for ISO 27001 implementation.

Step 2:- Information Security Policy & Objectives

Deliverables:-



Development of Information Security Policy and Objectives for the organization as per ISO 27001 standard.

- Work shop with Top Management / Middle Management on development of Information Security Policy.
- Work shop with Top and Middle Level Functional Management on development of Information Security Objectives and plan for achievement.

Step 3:- Gap Analysis / Risk Assessment



Deliverables:-

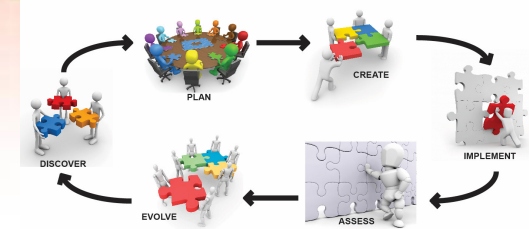
Identification of degree of compliance of existing system with requirements of ISO 27001 standard. Determination of how various organizational hazards impacts the information security.

- Understanding of all the operations of the organization.
- Carrying risk assessment for various processes of the organization. Identification of significant risks.
- Comparing existing operations with requirements of ISO 27001 standard.

Step 4:- Documentation / Process Design



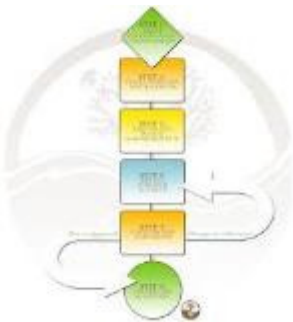
Deliverables:-



Documentation of the entire process as per requirements of ISO 27001 Information Security Management System.

- Information Security Manual
- Functional & mandatory Procedures
- Formats / Operation control plan
- Work instructions / Guidelines
- Legal register, Information Security training, accident / incident reporting, purchase, quality plans, etc.

Work-shop on design and development of documents as per ISO 27001 requirements.



Step 5:- Documentation / Process Implementation



Deliverables:-

Processes / Documents developed in the last module implemented across the organization covering all the departments and activities.

- Work–shop on process / document implementation as per ISO 27001 requirements.
- Departmental / Individual assistance in implementing the new processes / documents.
- Initiate Information Security performance monitoring system

Step 6:- Internal Audit



Deliverables:-

A robust internal audit system for the organization.

- Internal Auditor Training & Examination.
- Successful employees carry out internal audit of the organization covering all the departments and operations.
- Suggest corrective and preventive actions for improvements in each of the audited departments.

Step 7:- Management Review Meeting



Deliverables:-

A formal system of top management reviewing various business information security aspects of the organization.

- Review the Information Security management system to ensure its continued suitability, adequacy and effectiveness.
- This management review must be documented and must address the need for changes to the Information Security management system and assess opportunities for improvement.

....and develop action plan

Step 8:- Pre assessment Audit



Deliverables:-

A formal Pre Certification audit conducted to assess effectiveness of ISO 27001 implementation in the organization.

- A replica of final certification audit.
- Finds degree of compliance with ISO 27001 standard.
- Gives an idea to the employees about the conduct of the final certification audit.

Step 9:- Corrective – Preventive Actions



Deliverables:-

Organization ready for final certification audit.

- On the basis of pre-assessment audit conducted in the last step, all the non-conformities will be reviewed and our team will assist your employees to close by taking appropriate correction, corrective actions and identify preventive actions.
- A final review by our experts will ensure that all the NCs are closed effectively and the organization is ready for the final certification audit.

Step 10:- Final Certification Audit



Deliverables:-



Organization awarded ISO 27001 certification.

- You can select the certification body of your preference or else we can assist and suggest you the most appropriate certification body for your organization.
- We provide 100% onsite assistance and support to ensure smooth conduct and successful completion of audit.
- Upon the audit, your organization will be ***awarded ISO 27001 certification.***

Need More Information.....?

Sterling International Consulting FZE

Level 6, Office 605 - The Fairmont, Sheikh Zayed Road,
PO BOX 27363, Dubai, United Arab Emirates

Phone: +971 505842597

Email: info@uaeiso.com

Web: www.uaeiso.com

Web: www.uaeiso.com

