27001 Academy

Diagram of ISO 27001:2013 Implementation Process

Note: This diagram shows the steps for ISO 27001 (2013 revision) implementation and certification; it does not show the complete Plan-Do-Check-Act (PDCA) Cycle.

To learn more about ISO 27001 click here.

Obtain management support

Communication with interested parties + records of communication

Monitoring & measurement + records of results

Establish the project (not mandatory)	Project Plan (not mandatory)	Budget; Human resources plan

Identify requirements	List of interested parties, legal, regulatory and contractual requirements

Define scope, management intention, responsibilities	Information security policy + Scope document	Information security objectives

Implement support procedures	Procedures for document control, internal audit, corrective action (not mandatory)

Design the process of risk assessment and treatment	Risk assessment methodology	Risk acceptance criteria

Perform risk assessment and treatment	Risk assessment table	Risk treatment table	Risk assessment and treatment report

Develop a security profile of the company	Statement of Applicability

Accept residual risks & develop a plan for control implementation	Risk treatment plan	Acceptance of residual risks

Implement all required controls	Records of implementation

Perform training and awareness programs	Training records

Operate the ISMS	Various records required by ISMS documentation

Conduct internal audit	Internal audit report	Corrective actions

Management review	Management review minutes

Stage 1 certification audit (Documentation Review)	Stage 1 audit report	Corrective actions

Stage 2 certification audit (Main audit)	Stage 2 audit report	Corrective actions

Mandatory only for companies going for the certification

Courtesy of: 27001Academy www.iso27001standard.com

Copyright ©2013 EPPS Services Ltd