

ISO 27001:2005 Information Security Management System (ISMS)

With the immense corporate competitions, challenges and as businesses grow and expand across borders, transactions and business communications drastically leading to an exponential increase in the value of and dependency on information and processing facilities. Recent high profile information security incidents and breaches and the various laws and regulations framed to protect information, forcefully stress the ever-increasing need for organizations to establish and maintain information security measures.

Information Security Management Systems (ISMS) is a structured and systematic approach to manage sensitive and critical organization information so that it remains secure, correct and available all the time. ISO 27001 is an International Standard for 'Information Security' that specify requirements for establishing an institution-wide Information Security Management System for the protection of institution's valuable financial and technical information assets. This standard establishes the worldwide best security practices as the Information Security policies and procedures that eventually reduce the probability of internal and external attacks on Information Assets and also limit the damage caused by an inadvertent or malicious incident. ISO27001 certification is widely accepted, recognized and valued in the national and international markets.

ISO 27001 Consulting Services

Quest Consultants (QC) are the pioneers in Information Security Systems by being the FIRST consultancy firm in Pakistan with a successful proven track for ISO 27001 Information Security Management System (ISMS) certification. *Quest Consultants* are proud to be the ISO 27001 ISMS consultants for the first company in Pakistan that achieved the ISO 27001 ISMS certification in December 2006.

Quest Consultants has a panel of consultants that includes **ISO 27001 Lead Auditors** and IT professionals, possessing more than 13 years of IT and consultancy experience. QC also has 'Information Technology Advisor' on its panel of experts having expertise in the area of Networking, Database Management and Software Applications Development. Based upon our successful certification experience, **we guarantee ISO 27001 ISMS certification** to our clients.

Our ISO 27001 consulting services include the following:

- I. ISO 27001 ISMS Training Workshops
- II. ISO 27001 ISMS Auditing
- III. ISO 27001 ISMS Consulting (including training and auditing)
- IV. Other ISMS related services

I. ISO 27001 ISMS TRAINING WORKSHOPS

Awareness and 'correct' understanding / interpretation of the ISO 27001 ISMS standard requirement are the key factor in its effective implementation and successful certification. Therefore, comprehensive trainings workshops of this international security standard are considered as vital when undertaking the ISO 27001 implementation project. To suit the needs of differing client / audience, following are the types of corporate trainings devised and offered to the interested clients

Training Workshop 1: Executive Briefing Training Session

This is a 2 / 3 hours executive session specifically devised for the top management of the company. It focuses upon the key issues and interests related to the 'top management'. Following are some of the topics that are addressed in this session:

- Fundamentals to information security
- Why ISO 27001 is essential for Information Security
- ISO 27001 Information Security standard – an overview
- An overview of Information Assets, Risk Assessment, Business Impact Analysis, Business Continuity Planning and Disaster Recovery Planning

- Implementation roadmap for ISO 27001 Information Security standard
- Benefits to the organization
- ISO 27001 certification process
- Costs Involved

Training Workshop 2: Implementing Information security and Achieving ISO 27001 ISMS certification

This is a 2/3 full days professional training workshop designed for the top management, head of departments and personnel assigned the task of implementing and achieving ISO 27001 ISMS certification for their organization. This training course is aimed to provide detailed understating of the ISO 27001 standard requirements, proven ISO 27001 project implementation methodology leading to a successful certification. It is highly customized for the client organization with the objective of enabling the participants to implement Information security at their organization. Some of the topics it covers:

- Information Security, its importance, fundamentals and basics
- Proven Project Implementation Methodology
- Detailed explanation of the ISO 27001 ISMS Standard requirements and related ‘Security Controls’
- Risk Assessment – Methodology, Identification, Assessment and treatment of risks
- Business Continuity planning (BCP) and Disaster Recovery Planning (DRP)
- Development of Security Policies, Procedures/Systems and their implementation
- Roadmap to successful ISO 27001 certification

Practical Exercise on:

- Information Assets Inventories
- Risk Assessment Plan
- Business Impact Analysis & Risk Assessment of Business Processes
- Business Continuity Plan/Disaster Recovery Plan

This workshop is specifically designed and **guaranteed** to enable the participants to immediately start the implementation at their organization.

II. ISO 27001 ISMS AUDITING

This offering ensures compliance of the existing IT environment and its management procedures with the ISO 27001 controls and guidelines for the enterprise security posture. The audit comprises of the following modules:

- ISMS Audit
- Assets Audit
- Business Processes Audit
- Security Architecture Audit
- Policies Audit
- Procedures and Systems Audit
- Compliance Report

The auditing service can be acquired in the forms of 3 modules below:

Gap Analysis – done while undertaking the project of ISO 27001 implementation; to find the gap b/w the existing system at the company and the requirements for ISO 27001 ISMS certification

Documentation Audit – done to verify only the documentation compliance against the requirements of the ISO 27001 standard

External Pre Audit – done before certification to have the surety over the established ISMS system before engaging the certification agency for the final certification auditing

All the above audits are done by the experienced ISO 27001 Lead Auditor followed by an Audit Report detailing the information as per the selected module.

III. ISO 27001 ISMS CONSULTING (including Training and Auditing)

Consultancy service for ISO 27001 ISMS is the major service which incorporates the trainings and auditing services mentioned above. This turnkey solution is based upon the deployment of our experienced ISO 27001 consultant on the project site who develops the complete documentation and facilitates its implementation till successful ISO 27001 ISMS certification. The key steps of the consultancy process are:

- Gap Analysis of the company against the ISO 27001 ISMS standard requirements
- Training of the management over the ISO 27001 ISMS standard
- Compilation of Information Assets Inventories
- Risk Assessment- Information Assets
- Creation of an ISMS Framework
- Business Continuity Planning (BCP)
- Disaster Recovery Planning (DRP)
- Security Policies and procedures
- Security Procedures Deployment & Implementation
- Information Security Manual
- Testing drill exercises for BCPs and DRPs
- Training of the company selected personnel as 'Internal Security Auditors' for the ISO 27001 standard
- Internal Security Audit and preparation for the final certification audit

The above sequence of QC is based upon the successful certification process. Complete guidance is provided through out the process along with guaranteed ISO 27001 certification

IV. OTHER ISMS RELATED SERVICES

For clients interested in addressing specific areas of the information security / business continuity at their companies, following are the ISMS related service modules developed and provided as per the company requirements. These services also fulfill the specific requirements of the ISO 27001 Information Security Management System standard:

- **Information Security Manual** (it outlines the security policies and a brief about the possible information security procedures and mechanisms as per the trade and business operations of the client company)
- **Documentation for ISO 27001** (it includes the development of all the documents and procedures as per the business/trade of the client company that are required to comply with this International Standard)
- **Information Assets Inventories, their Risk Assessment Plan with Risk Treatment Plan** (it is done for all the information assets exist at the client company)
- **Business Continuity Management including Business Impact Analysis, Risk Assessment Business Process and the Disaster Recovery Planning** (it is done for all the processes at the client company)

These services can be acquired in isolation or in combination depending upon the requirement from the client company.

CONSULTANCY CHARGES

The schedule of charges for all the above mentioned services can be acquired by calling at (021) 4537601 / 4537682