Information Guide

PQSmitra
Simple & Practical

ISO/IEC 27001:2022 Information Security Management System (ISMS)

Corporate Office:
Office No. 7 & 8, Ashok Nagar 1 B,
Vazira, Borivali (W), Mumbai – 400 092.
Maharashtra, INDIA

+91 98202 04373 / 98200 33608
info@pqsmitra.com
www.pqsmitra.com

What is ISO 27001?

ISO/IEC 27001 Information security management system is an internationally recognized standard, which can be applied / implemented to any organization irrespective of sizes, production or services industries. It also covers all the industries or markets. Information security management system was drawn up by the International Organization for Standardization (ISO), with intent to set international requirements for Information Security Management System.

According to the definition “ISO 27001 standard is developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the Information Security Management System (ISMS)”. In today’s world of business, information is a life support system for any organization. But organizations system for securing the information is exposed to various kinds of security threats i.e., computer assisted fraud, spying, damage or destroying of data, damage to property, fire or flood. The most common are computer viruses, hacking etc., which have become more common and increasingly sophisticated.

ISO 27001 is a determination for an information security management system, a framework of activities and policies concerning the management of information risks. ISMS is utilized by the organizations to identify, analyze and address its information risks and guarantees that the security arrangements are adjusted to keep pace with changes to the security dangers, vulnerabilities and business impacts

What are the Focus Points of ISO/IEC 27001:2022 Implementation?

ISMI 27001:2022 requires that management:

- Ensuring Information Security within Organization
- Ensure Cyber & Cloud Security within Organization
- Ensuring Risk Assessment & Treatment
- Ensuring Confidentiality, Integrity & Availability of IT resource
- Standardization of IT processes

Who all are eligible for ISO 27001 Certification?

The organizations requiring robust controls with regards to Confidentiality, Integrity and Availability of the data can implement ISO 27001 ISMS. Generally the organizations from the field of Information

- Technology,
- Research,
- Development,
- Design Services,
- Financial services

Can avail ISO 27001 certification. In most of the cases, it is a specific requirement stated by their customer.

How will ISO/IEC 27001 Certification Benefit your Organization?

- Ensuring Confidentiality, Integrity and Availability of data
- Reduces the Risk of Cyber Attacks
- Ensuring Information Security within Organization
- Satisfaction and Retention of Valuable Customers
- Compliance with business, legal, contractual, and regulatory requirements
- Improved structure and focus with respect to information security

How did ISO 27001 ISMS evolve throughout the year?

- Year 1992 – Code of practice for security management
- Year 1995 – British Standard Institute (BSI) BS 7799
- Year 2000 – ISO/IEC 17799
- Year 2005 – ISO/IEC 27001:2005 (Information security management system) Published
- Year 2013 – 1st Revision of the standard
- Year 2022 – 2nd Revision of the standard

ISO/IEC 27001:2022 Reference Standards

- ISO 9000:2015 - Quality management - customer satisfaction - Guidelines for complaint handling in organizations
- ISO 27002 - ISMS controls (Information Security Management System)
- ISO 27003 – ISMS Implementation guidelines
- ISO 27004 – ISMS Measurements
- ISO 27005 – Risk Management

What is ISO 27002:2022?

- ISO 27002 provides detailed Guidance on implementing the Controls that can be selected in an ISMS based on ISO 27001.
- 2022 edition now titled "Information security, cybersecurity and privacy protection - Information security controls"
- Restructure the controls in ISO 27002:2022
- It cannot be used for Third Party Certification because it is a guideline.

What is the validity of the ISO 27001 Certification?

- The validity period for an ISO 27001 standard is 3 years with an annual surveillance audit for monitoring the ISMS.

What are structural changes in ISO 27001?

- There are a number of structural changes including the addition/ modification of some of the sub-clauses
- Clause 4.2 (c) in which needs and expectations of interested parties will be addressed by the ISMS
- Clause 6 (now includes a sub-clause 6.3)
- Clause 9.2 now has 2 sub-clauses
- Clause 9.3 now has 3 sub-clauses
- Clause 10 has been restructured

How will PQSmitra help you with Hassle Free Implementation process for ISO/IEC 27001 ISMS Certification?

PQSmitra adopts a result-oriented approach for the effective information security management system implementation at the organization. PQSmitra team offers assistance in framing “Statement of applicability” also for documenting the various procedures for compliance purpose and implementation. PQSmitra offers 100% documentation support to achieve successful certification in addition to enhanced operational controls. The implementation process is described below:

- Initial visits & review of the existing system
- Statement of applicability
- Identification of controls and planning for implementation
- Training and Hand holding/ support for implementation
- Internal audit for verification of implemented system
- Management review
- Certification audit – Stage 1 & Stage 2
- Closure of non-conformities
- Rewarding the certificate to the organization

PQSmitraService Features appreciated by clients

Simple & Practical Approach

21 Years of Service

2500+ Successful Projects

5,56,000+ Consulting Hours

PQSmitra

Simple & Practical

Corporate Office:
Office No. 7 & 8, Ashok Nagar 1 B, Vazira, Borivali (W), Mumbai – 400 092.
Maharashtra, INDIA

+91 98202 04373 / 98200 33608 info@pqsmitra.com www.pqsmitra.com