INTERNATIONAL CERTIFICATION SERVICES

Information Security Management System (ISMS)

INFORMATION SECURITY MANAGEMENT SYSTEM

Why do I need ISMS ?

Recent information security breaches and the value of information are highlighting the ever increasing need for organization to protect their information. An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems.

Information is critical to the operation of all organizations and perhaps even the survival of all organizations. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by mail or by electronic means, shown in films, presentations, or spoken in conversation. In today's competitive business environment, such information is constantly under threat from many sources. These can be internal, external, accidental or malicious. With the increased use of new technology to store, transmit, and retrieve information, we have all opened ourselves up to increased numbers and types of threats and vulnerabilities. Being certified to ISO/IEC 27001 will help you to manage and protect your valuable information assets.

ISO/IEC 27001 is the only auditable international standard which defines the requirements for an Information Security Management System (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls. This helps you to protect your information assets and give confidence to any interested parties, especially your customers. The standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving your ISMS on a continual basis.

Who Need it ?

ISO/IEC 27001 is suitable for any organization, large or small, in any sector or part of the world. The standard is particularly suitable where the protection of information is critical, such as in the finance, health, public and IT sectors. ISO/IEC 27001 is also highly effective for organizations which manage information on behalf of others, such as IT outsourcing companies. It can be used to assure customers that their information is being protected.

Information Security Management System an overview ?

ISO/IEC 27001:2005 is a standard setting out the requirements for an Information Security Management System. It helps identify, manage and minimize the range of threats to which information is regularly subjected. The standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties including an organization's customers.

It is suitable for different types of organizational use, including the following:

- Formulation of security requirements and objectives;
- To ensure that security risks are cost effectively managed;
- To ensure compliance with laws and regulations;
- As a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- Identification and classification of existing information security management assets;
- To be used by management to determine the status of information security management activities;
- To be used by internal and external auditors to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- To provide relevant information about information security policies, directives, standards and procedures to trading partners;
- To provide relevant information about information security to customers.

How to go about ISO/IEC 27001:2005 Certification *for Information Security Management System ?*

- Define the scope and boundaries of the ISMS. An ISMS can cover all or part of an organization.
- Define and document Security / ISMS Policy. This document addresses the issues like Why is information security important to you ? Is there a particular threat, or other vulnerabilities that concern you ? What do you want to achieve, for example in terms of confidentiality, integrity and availability ? What do you believe is an acceptable level of risk? Are there constraints, such as laws and regulations, or particular ways in which you wish to do things? and so on.
- Plan and carry out Risk Assessment.
- Develop the Risk treatment plan.
- Select control objectives and controls. ISO 27001 presents a list of control objectives and controls, drawn one-to-one from ISO/IEC 17799:2000. The list is not exhaustive and the organization is free to identify additional control objectives and controls as appropriate. Not all of those listed in ISO 27001 may also be relevant.
- Prepare a Statement of Applicability (SOA). The SOA is a document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of Risk Assessment and risk treatment processes.
- Obtain management approval on the proposed residual risks and authorization to implement and operate the ISMS.
- Implement the above to the PDCA cycle by subjecting it to internal audits and management review there by applying improvements.

Benefits of Information Security Management Systems :

Certifying your ISMS against ISO/IEC 27001 can bring the following benefits to your organization:

Commercial Credibility, Trust and Confidence

Your customers can feel confident of your commitment to keeping their information safe. Registration can help set a company apart from its competitors in the marketplace. Demonstrates the independent assurance of your internal controls, meets corporate governance and business continuity requirements. Independently verifies that your organizational risks are properly identified, assessed and managed, while formalizing information security processes, procedures and documentation.

Cost Savings

The cost of a single information security breach can be significant; the cost of several could be catastrophic. An ISMS reduces the risk of such costs being incurred and this is important to stakeholders and other investors in your business. Possible reduction in insurance premiums can also be realized.

Legal Compliance

Registration demonstrates to competent authorities that the organization observes all applicable laws and regulations. In this matter, the standard complements other existing standards and legislation. Independently demonstrates that applicable laws and regulations are observed.

Commitment

Registration helps to ensure and demonstrate commitment at all levels of the organization. Provides a competitive edge by meeting contractual requirements and demonstrating to your customers that the security of their information is paramount.

Operating Level Risk Management

Leads to a better knowledge of information systems, their weaknesses and how to protect them. Equally, it ensures a more dependable availability of both hardware and data.

Employees

Improves employee awareness of security issues and their responsibilities within the organization. Proves your senior management's commitment to the security of its information.

Continual Improvement

Regular assessment process will help you to continually use, monitor and improve your management system and processes.

Are you looking for ISMS Certification ?

Call for further information at :

International Certification Services Pvt. Ltd.

Corporate Office

22/23, Goodwill Premises, Swastik Estate, 178 CST Road, Kalina,
Santacruz (E), Mumbai- 400 098, Maharashtra, INDIA.

Tel : 022-26507777-82, 42200900, 30608900-4, **Fax:** 42200933,

Email : info@icspl.org / info@icsasian.com **Web:** www.icsasian.com / www.icspl.org

Rev.1/15.10.2010

INFORMATION SECURITY MANAGEMENT SYSTEM