



LAKSHY

Lakshy Management Consultant Pvt. Ltd.

ISO 27001:2005

Information Security Management System

If your information is not safe,
the future of your business is not secure

Web: www.lakshy.com E-Mail: info@lakshy.com



What Is ISO 27001?

- ISO 27001, titled "Information Security Management - Specification With Guidance for Use", is the replacement for BS7799-2. It is intended to provide the foundation for third party audit, and is 'harmonized' with other management standards, such as ISO 9001 and ISO 14001.
- An Information Security Management System (ISMS) is a management system based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. It is an organizational approach to information security. ISO/IEC 27001 (BS 7799) is a standard for information security that focuses on an organization's ISMS.

Objective of ISMS

- Information security is the protection of information to ensure:
 - Confidentiality: ensuring that the information is accessible only to those authorized to access it.
 - Integrity: ensuring that the information is accurate and complete and that the information is not modified without authorization.
 - Availability: ensuring that the information is accessible to authorized users when required.



Why should I implement ISO 27001 ISMS?

- Certification of a management system brings several advantages. It gives an independent assessment of your organization's conformity to an international standard that contains best practices from experts for ISMS. A certified ISMS does not guarantee compliance with legislative and local policies, but provides a systematic platform to build on.
- Drivers for certification include:
- Meeting U.S. legislative requirements directly:
 - Sarbanes-Oxley Act of 2002, Section 404
 - SAS/70 requirements
 - HIPAA requirements (Security rule)
 - Gramm Leach Bliley Act of 2002
 - California's privacy laws including SB 1436

Why should I implement ISO 27001 ISMS?

- Meeting legislative and regulatory requirements indirectly:
 - Privacy legislation
 - Managing the need to meet international legislative requirements
- As part of a supplier management program:
 - Some major corporations prefer suppliers that can prove they meet best-practice standards.
 - In some industries, certification is demanded by customers. This is often seen in finance related industries, data centers, and online service providers.

Why should I implement ISO 27001 ISMS?

- As a measure and independent evidence that industry best practices are being followed.
- To reduce insurance premiums:
 - In some cases insurance premiums can be reduced if you can prove that you meet the best practice standards
- As part of a corporate governance program
 - Corporations must take care to meet the best practices and often need to show stakeholders such as sponsors, shareholders, and financiers that they take good care of information security.
- Offers competitive advantage; ISO/IEC 27001 (BS 7799) certification might be a differentiating factor between you and your competition.



Main concepts of ISO/IEC 27001 ISMS

- All activities must follow a method. The method is arbitrary but must be well defined and documented.
-
- The standard requires a company to specify its own security goals. An auditor will verify whether these requirements are fulfilled.
- All security measures shall be the result of a risk analysis.



Main concepts of ISO/IEC 27001 ISMS

- The standard offers a set of security controls. It is up to the organization to choose which controls to implement based on the specific needs of their business.
- A process must ensure the continuous verification of all elements of the security system through audits and reviews.
- A process must ensure the continuous improvement of all elements of the security system.

Process for implementing ISO 27001

- 1) Define an information security policy
- 2) Define scope of the information security management system
- 3) Perform a security risk assessment
- 4) Manage the identified risk
- 5) Select controls to be implemented and applied
- 6) Prepare an SoA (a "statement of applicability").

Security policy

- Establish a security policy.
- State management commitment to the policy.
- Give a brief description of security principles, standards and compliance requirements.

Security organisation

- Controls specifying allocation of individual security responsibilities.
- Deals with need for specialist security knowledge.
- Concerns information systems relationships with outside parties such as contractors, partners and outsourcing companies.

Asset classification and control

- Requires the compilation of an inventory of all information systems assets.
- Details of ownership, location and importance also to be included.
- Requires software licences for all operating system and application software to be current.

Personnel security

- Specifies the proper screening and checking of employee details at the time of hiring.
- Places importance on user training in security matters.
- Emphasises importance of reporting security incidents.

Physical and environmental security

- Seeks to establish what physical access controls are in place.
- Controls included to protect equipment from environmental hazards.
- Requires "clean desk policy" for locking away of sensitive information.

Access control

- Requirement for a general-access control policy.
- Seeks to establish how access authorisation is granted.
- Reviews how access of systems is monitored.

Communications and operations management

- Seeks to establish if network security controls are in place.
- Includes controls for system planning and acceptance.
- Incorporates procedures for handling of media.

Systems development and maintenance

- Details controls that can help build security into systems developed in-house.
- Controls included on use of cryptography.
- Requirement for change control is addressed.

Business continuity management

- Describes processes for ensuring business continuity.
- Details plans to be developed to maintain or restore business operations.
- Provides a framework for the formation of these plans.

Compliance

- Comprises controls specifying the need to comply with legal standards.
- Seeks to establish if there is a security testing programme in place.
- Establishes if back-ups are carried out effectively and if they are tested.

ISO 27001:2005 Awareness

Need More Information.....?



Lakshy Management Consultant Pvt. Ltd.

232, Sai Chambers, Sector 11, CBD Belapur,
Navi Mumbai 400 614, India

Phone: +91 22 32995241

24 Hour Customer Care: +91 9821780035

Email: info@lakshy.com

Web: www.lakshy.com