



## **ISO 27001:2005**

# **Information Security Management System**

---

ISO 27001:2005 is an 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. The standard is particularly suitable where the protection of information is critical, such as in the finance, health, public and information technology sectors. The confidentiality, integrity, and availability of vital corporate and customer information are essential to maintain competitive edge, profitability, legal compliance and commercial image. Implementing an ISO 27001:2005 information security management system allows your organization to enforce information security and reduce the possible risk of fraud, and information loss or information disclosure.

The ISO/IEC 27000-series comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The series provides best practices on information security management, risks, and controls within the context of an overall Information Security Management System. The standard is similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

The ISO 27001:2005 Information Security Management Systems (ISMS) certification enables you to demonstrate your commitment to information security and customer satisfaction, as well as continuously improving your corporate image. The standard is made of documents:

- ISO 17799: Guidance on implementing ISMS.
- ISO 27001: Standard against which ISMS can be certified.

The first step is to define the scope of the ISMS policy. This is critical to identify the potential dangers you face and decide a systematic approach to how to assess these risks. A successful ISMS includes standard steps for implementation, operation, review, and maintenance.



The ISO 27001:2005 standard encompasses the following twelve sections:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations
- Management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

## **Benefits of ISO 27001:2005**

Registration to this internationally recognized standard enhances any company's credibility. It clearly demonstrates the validity of your information and a real commitment to upholding information security. The establishment of an ISMS can also transform your corporate culture both internally and externally, opening up new business opportunities with security conscious customers and clients. In addition improving employee ethics and the culture of confidentiality throughout the enterprise.

Further benefits include:

- Provides policies & procedures in accordance with internationally recognized criteria, structure and methodology
- Provides confidence that you have minimized risk in your own security program
- Can be a deciding differentiator in contract negotiations
- A defined process for implementation, management, maintenance and ISMS evaluation
- Increased security delivers lower costs: fraud, inefficiency and errors reduced
- Compliance advantages for participation in Global business opportunities

[www.sustainingedge.com](http://www.sustainingedge.com)

Toll Free 888-572-9642