Management System

A Management System is the framework of processes and procedures used to ensure that an organisation can fulfil all tasks required to achieve its policies and objectives. Documented information ensures that everyone is not just "doing his or her thing", that there is a defined way to complete each of the business process organization has planned effectively and efficiently utilizing available resources. Management system ensures that all personnel are aware of their roles, responsibility for effective implementation of process including continual improvement.

Planned Information Security Management System (ISMS) formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. ISMS preserves the confidentiality, integrity and availability of information by applying a risk management process, thus giving confidence to interested parties that risks are adequately managed.

Concept of Risk-based thinking enables an organization to determine the factors that could cause its processes and its information security management system to deviate from the planned results, to put in place preventive controlsto minimize negative effects and to make maximum use of opportunities as they arise. Risk being the effect of uncertainty, thus (any uncertainty) results in having positive or negative effects. A positive deviation arising from a risk can provide an opportunity, but not all positive effects of risks results in opportunities.
Organisations that claim to have adopted ISO 27001 can therefore be formally audited and certified compliant with the standard.

ISO 27001 requires that management:

- Systematically examines the organisation's information security risks, taking account of the threats, vulnerabilities, and impacts.
- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable.
- Adopts an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an on-going basis.

Reasons to go for ISO 27001 Certification:

Primary reasons:

- Improve interested parties' trust by assuring compliance with their requirements
- Improve marketing edge (image and credibility) by attaining certification to ISO 27001
- Reduce expenses related to information security incidents
- Improve internal organization by better defining responsibilities and duties

Secondary reasons:

- Integrate information security to business process for better alignment
- Improve decisions by basing them on data from the information security management system
- Create a culture of continual improvement of the information security
- Improve employee, and other interested parties', engagement in information security improvement

Benefits of ISO 27001 – Information Security Management Systems

- Business' security risks are managed cost-effectively
- Sends a valuable and important message to customers and business partners that this business does things the correct way
- It demonstrates a clear commitment to Information Security Management to third parties and stakeholders
- It can provide a framework to ensure the fulfilment of commercial, contractual and legal responsibilities
- It provides a significant competitive advantage, and can effectively be a license to trade with companies in certain regulated sectors
- It provides for inter-operability between organisations or groups within an organisation
- It can provide compliance with, or certification against, a recognised external standard which can often be used by management to demonstrate due diligence.

How to achieve compliance to ISO 27001 requirements:

- Defining the ISMS framework
- Identifying the current risk scenario
- Selecting and implementing proper security controls
- Providing proper awareness, training, and education to the users
- Providing relevant information to management for the first critical review of the ISMS for continual improvement