Introduction to ISO/IEC 27000

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization

by

Sudhanwa Jogalekar

Sudhanwa Jogalekar

- Qualifications: BE, DBM, MCM, (Dip cyberlaw)
- Professional certification: ISO 27001 Lead Auditor
- Professional experience : 25 years
- Academic experience: Syllabus design, paper setting, assessments, QIP, teachers training programs, visiting faculty etc. for Pune, Symbiosis University
- FOSS evangelist. Promoting FOSS for 10 years. Conduct FOSS workshops, seminars, training programs, conferences etc.

Various Standards

- ISO 9000 (QMS)
- ISO 14000 (EMS)
- ISO 27000 (ISMS)
- ISO 20000 (IT SMS)

ISO 27000 family

- ISO/IEC 27001 formal ISMS specification
- ISO/IEC 27002 infosec controls guide
- ISO/IEC 27003 implementation guide
- ISO/IEC 27004 infosec metrics
- ISO/IEC 27005 infosec risk management
- ISO/IEC 27006 ISMS certification guide
- ISO/IEC 27011 ISO27k for telecomms
- ISO/IEC 27033-1 network security
- ISO 27799 ISO27k for healthcare

ISO 27000 Basics

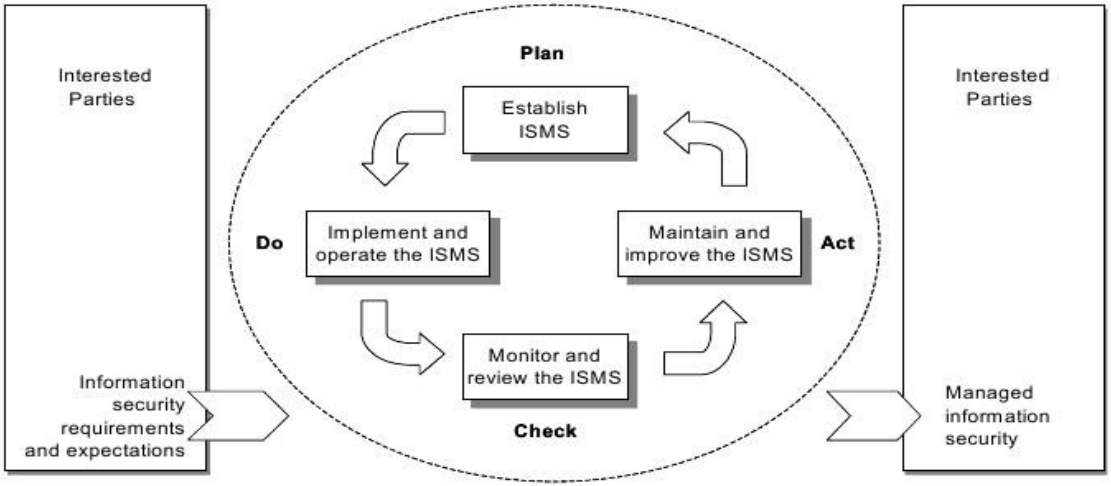


Figure 1 — PDCA model applied to ISMS processes

Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

Why ISO 27001?

- **ISO/IEC 27001 is an investment in the company's future**

- A "risk based" management system to help organisations plan and implement an information security management system (ISMS),assists organisations by providing a structured and a proactive approach to information security, by making sure the right people, processes, procedures and technology are in place to protect information assets.

- Help minimise possible harm to organisations that can be caused by deliberate or accidental acts.

Why ISO 27001?

- Framework that will take account of all legal and regulatory requirements.
- Gives the ability to demonstrate and independently assure the internal controls of a company (corporate governance)
- Proves senior management commitment to the security of business and customer information
- Helps provide a competitive edge to the company
- Reduces the amount of time and effort when audited by internal compliance reviews or external audits
- Easier to obtain funding and resources for information security team and security objectives

Why certification?

- Provides a goal, which will help facilitate the implementation of an information security management system and security controls
- Formalizes, and independently verifies, Information Security processes, procedures and documentation
- Independently verifies that risks to the company are properly identified and managed
- Help identify and meet contractual and regulatory requirements
- Demonstrates to customers that security of their information is taken seriously

Certification

- Standard
- Policies
- Regulations
- Mandatory
- Best practices

Certification

- Management Support
- Staff support
- Technical support
- Vendor support – SLA, NDA
- Best practices

Information Security V/S IT Security

- User desktops
- Manager laptops
- Servers
- LAN, WAN
- Server room A/C
- Company bus/car drivers
- Security guard at reception
- Routers
- Fire extinguishers
- Canteen
- Software licenses

ISMS and Asset Management

ISMS is “Management assurance mechanism for security of business information assets from potential security breach.”

It relates to all types of information, be it paper based or electronic.

Secure information is one that ensures Confidentiality, Integrity and Availability.

Confidentiality: ensuring that information can only be accessed by those with the proper authorization

Integrity: safeguarding the accuracy and completeness of information and the ways in which it is processed

Availability: ensuring that authorized users have access to information and associated assets when required

ISMS and Asset Management

"Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected."

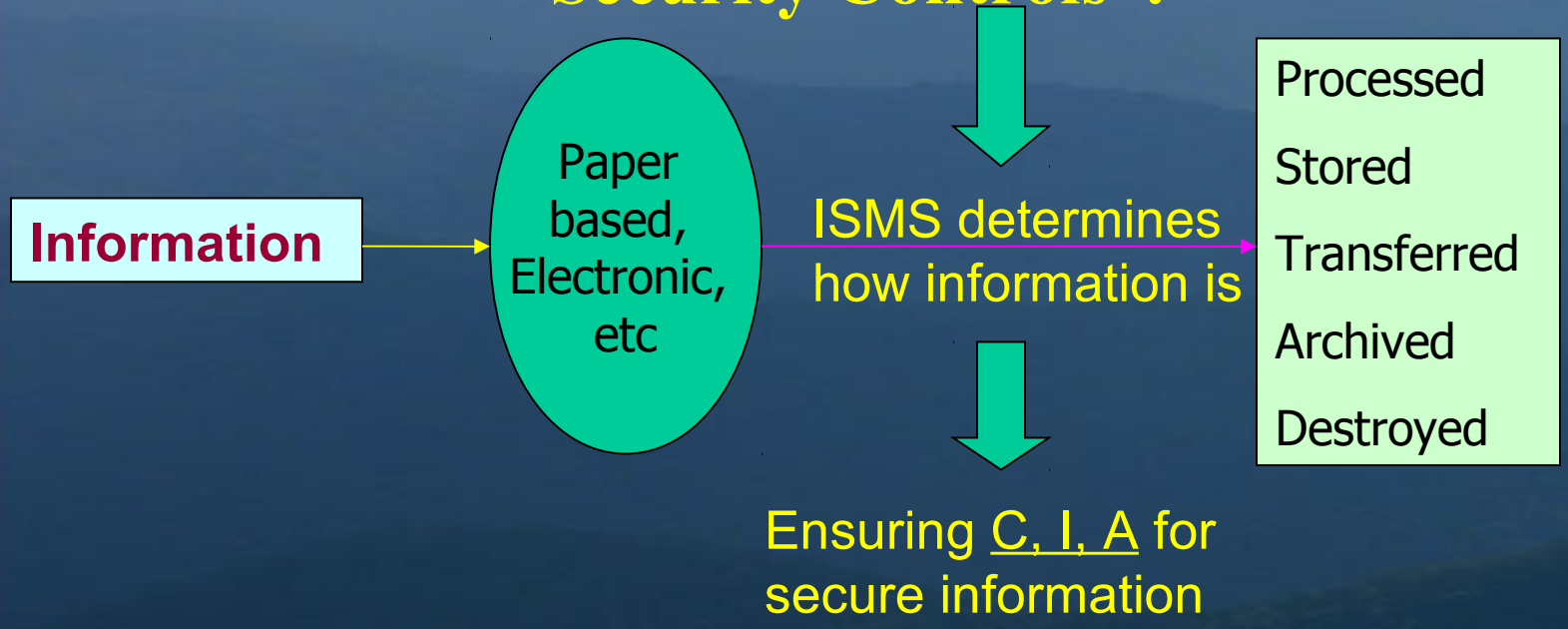
Asset is something that has "value".

Information assets of an organization:
Business data, Employee information, Research records
Price lists, Tender documents

Organization must determine which assets can materially affect the delivery of product/service by their absence or degradation

Information Security…

"Information Security is about protecting Information through selection of appropriate Security Controls".



To protect information assets from potential security breach

Assets and RA/RTP

- Risk Assessment
- Risk Treatment Plan
- Continuous Improvement
- PDCA
- Audit process

ISO 27001 standard

- **Clause 4:** Information Security Management System
- **Clause 5:** Management Responsibility
- **Clause 6:** Internal ISMS Audit
- **Clause 7:** Management Review of the ISMS
- **Clause 8:** ISMS Improvement
- **Annexure A:** Domain, Control Objective & Controls

11 Domains

Introduction to ISO/IEC 27000

??? Questions ???

Coming up
Part II (Implementation)