Information Security Management System
ISO 27001:2005

What is information security?

"Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities"

Information Security …….

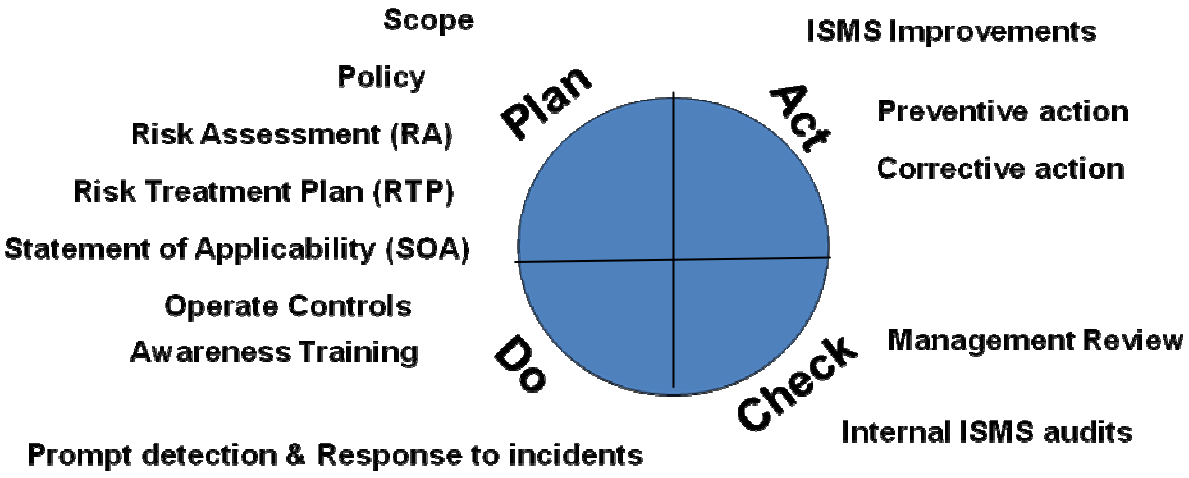
"Security has to move away from being a technology issue and bacome a business related issue."

"Ensures business continuity, minimises business damage, through the management of information security risks & maximizes business opportunities"

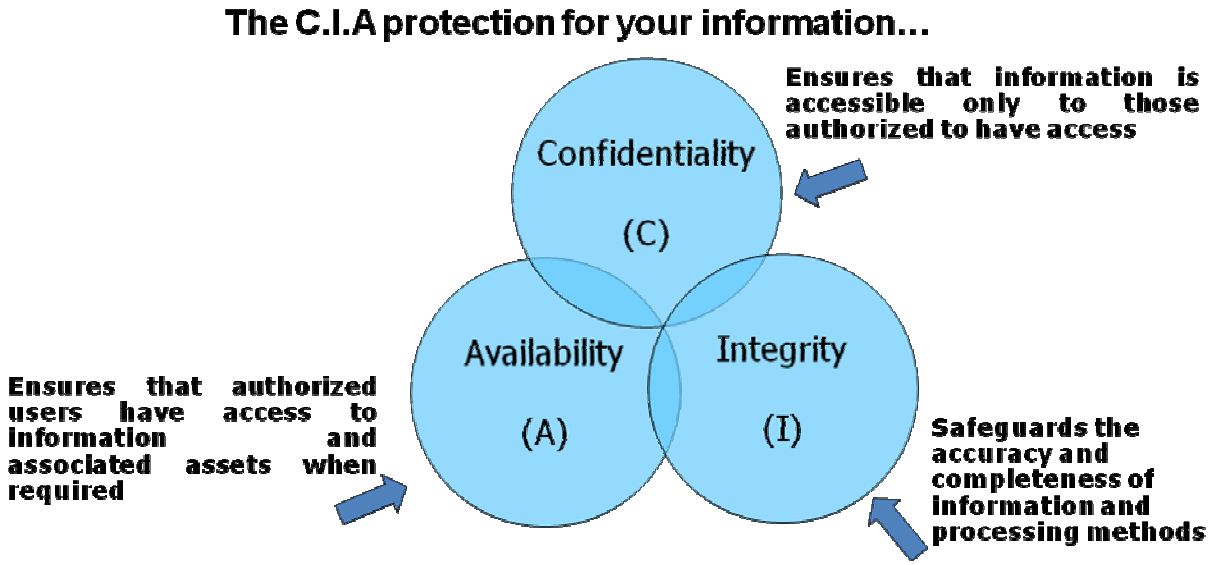
"There is a risk aspect to security too. Security breaches create a risk for the enterprise. So it's not just about hardware and software solutions"

"Security is now essential since it has become a business enabler. Enterprise security should involve employees at all levels, customers & all entities that deal with the organization."

Principal Components of ISO 27001:2005



Information Security Management System
ISO 27001:2005



ISMS Comprises of two parts….

ISO 27001:2005
(Information Technology – Security Techniques –
Information Security Management Systems– Requirements)

ISO 27002:2005 (formerly ISO 17799:2005)
(Information Technology – Security Techniques – Code of
Practice for Information Technology Security Management System)

ISO 27001:2005 is divided into 11 main sections (Annexure A)

1 <u>Security Policy</u> :
Explains what an information security policy should cover and why each business should have one

Information Security Management System
ISO 27001:2005

2 Organizational Security :
Explains how information security management is organized

3 Asset Management :
Considers information & information processing equipment as valuable assets be managed and accounted for.

4 Human Resources :
Details any personnel issues such as training, responsibilities, vetting procedures, and how staff responded to security incidents.

5 Physical and Environmental Security :
Physical aspects of security including protection of equipment and Information from physical harm, as well as physical control of access to information & equipment

6 Communications and Operations Management:
Examines correct management and secure operation of information processing facilities during day-to-day activities

7 Access Control :
Control of access to information/systems on the basis of business/ security needs

8 Information System Acquisition, Development & Maintenance :
Designing and maintaining systems so that they are secure and maintain information integrity

9 Information Security Incident Management :
Concerned with ensuring information security events & weaknesses are communicated in a way which allows corrective action to be taken

Information Security Management System
ISO 27001:2005

10 Business Continuity Management :

Maintenance of essential business activities during adverse conditions, from coping with major disasters to minor, local issues

11 Compliance :

Business compliance with relevant national and international laws, professional, standards & any processes mandated by ISMS

The Approach to information security ……..

Risk management

Risk management is the process of identifying, analyzing, assessing, evaluating and reducing risk to an acceptable level and implementing the right defense mechanisms to maintain acceptable level of risk.

Risk management is a detailed process of identifying facets that could damage data, evaluation of those facets in light of data value and countermeasure cost, implementing cost – effective solutions for mitigating risk (s).

Importance of Risk management

It allows the managers to balance the operational and economic costs and achieve gains in mission capabilities.

It helps organization to assess and understand the business impacts current risk level and to prioritize future directions / recommendations

It helps organizations to evaluate options for treatment of risk by implementing appropriate controls, accepting risks, avoiding risk and transferring risk

Information Security Management System
ISO 27001:2005

Benefits of ISO 27001:

- Reduced operational risk
- Increased business efficiency
- Assurance that information security is being rationally applied
- Security awareness amongst staff and managers
- Certification can also be used as marketing initiative, assurance to business partners & clients.