

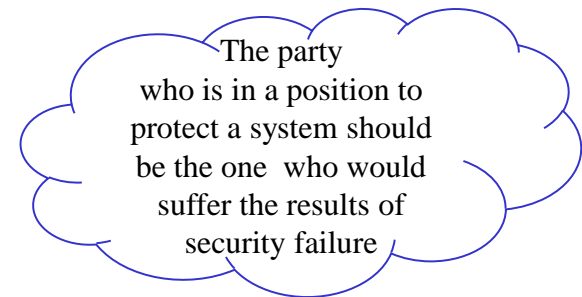
Is the issue of security and compliance a black art?

Bharathi Vasanthakrishna
May 20 2010

Definition

Information security means to control access, prevent damage to the information assets and ensuring secure and smooth business operations.

Information security includes protection of information at logical, physical and organizational levels



The party who is in a position to protect a system should be the one who would suffer the results of security failure

Threats



Can any of the following act as a threat to smooth business operations

- Job insecurity, dissatisfaction
- Virus outbreaks
- Volcanic ash
- Hardware failure and unavailability
- Memory stick
- Salami techniques



Can economics be viewed as a threat to IT security?

Brief History of ISO 27001

- BS7799 Part 2 in 1999
- Became ISO27001 in 2005
- Full name: ISO/IEC 27001:2005 -
- Information technology - Security Techniques - Information security management systems - Requirements
- Intended to be paired with ISO 27002

Elements of Information Security

Confidentiality

Protecting sensitive information from unauthorized disclosure or intelligible interception

Integrity

Safeguarding the accuracy and completeness of information and information systems

Availability

Ensuring that information and standard IT services are available when required

Information Security is preservation of Confidentiality, Integrity and Availability

Demystifying the elements



1. What if an intruder or another employee of a lower access level gets to read confidential top management mails?

This is a security breach in terms of -----

2. What if an intruder or another employee tries to modify the contents of the mail and the mail delivered is something different. For ex: The CEO sends out a mail to the CFO to donate GBP 1000 for a charity. Someone in between tampers the mail and changes the amount to GBP 3000 and give his account number.

This is a security breach in terms of -----

3. What happens if there is a hardware failure and the server is not available to the organization...???

This is a security breach in terms of -----



Demystifying the elements



1. What if an intruder or another employee of a lower access level gets to read confidential top management mails?

This is a security breach in terms of **Confidentiality** -----

2. What if an intruder or another employee tries to modify the contents of the mail and the mail delivered is something different. For ex: The CEO sends out a mail to the CFO to donate GBP 1000 for a charity. Someone in between tampers the mail and changes the amount to GBP 3000 and give his account number.

This is a security breach in terms of **Integrity** -----

3. What happens if there is a hardware failure and the server is not available to the organization...???

This is a security breach in terms of **Availability** -----

Why Information Security?

- Microsoft on Friday was urging Windows users to exercise caution as it looks for a way to close a security breach that exposes Windows users to viruses through emails and web sites.
- An outsourcing company in India is claiming to be an intermediary in an audacious deal that would involve inmates at Cherlapally Central Jail in Hyderabad, India, helping to process bank paperwork on behalf of two high profile western financial institutions.
- Heartland processes about 100 million card transactions each month, and it's not yet clear exactly how much fraud was committed when cyber-crooks tapped into Heartland's payment network. Visa and MasterCard, as well as some banks, have indicated fraud can be traced back to the Heartland breach Heartland Payment Systems .The security breach it has cost the company about US\$12.6 million so far
- Nato faces cyber attack threat

How to secure Information?

Integrity

Information is sufficiently right for the purpose at the time of use

Availability

Information is Accessible Wherever and Whenever Required

Confidentiality

Information is Available only to those Who are Authorised to Access it

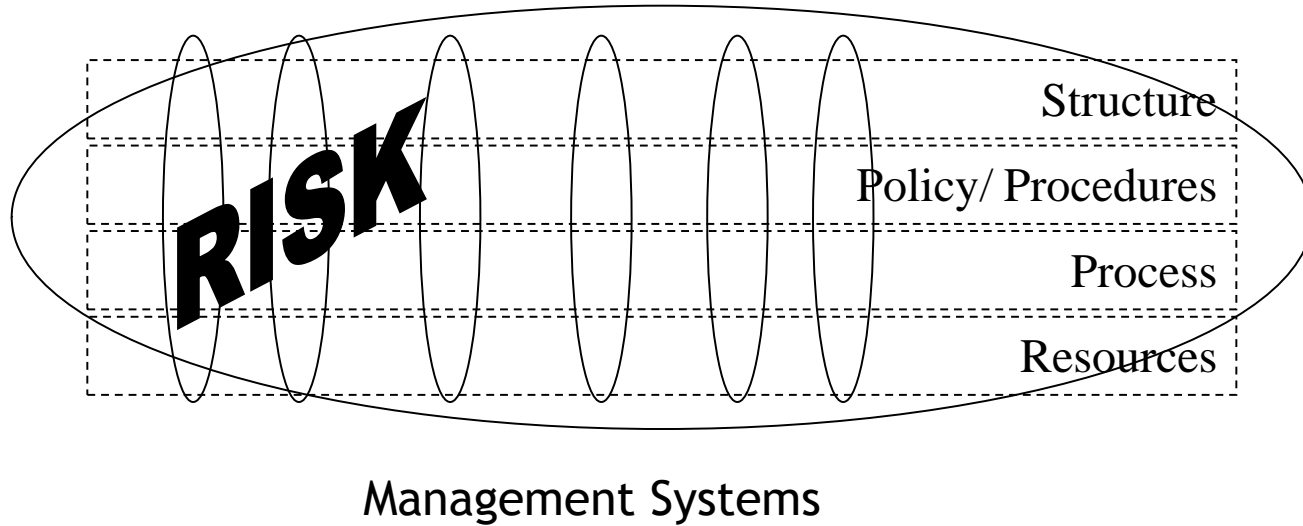
Is achieved by implementing a set of controls which could be policies, procedures, organizational structures and software function

Why Information Security?

- Protects information from a range of threats
- Ensures business continuity
- Minimizes financial loss
- Optimizes return on Investment
- Increases business opportunity

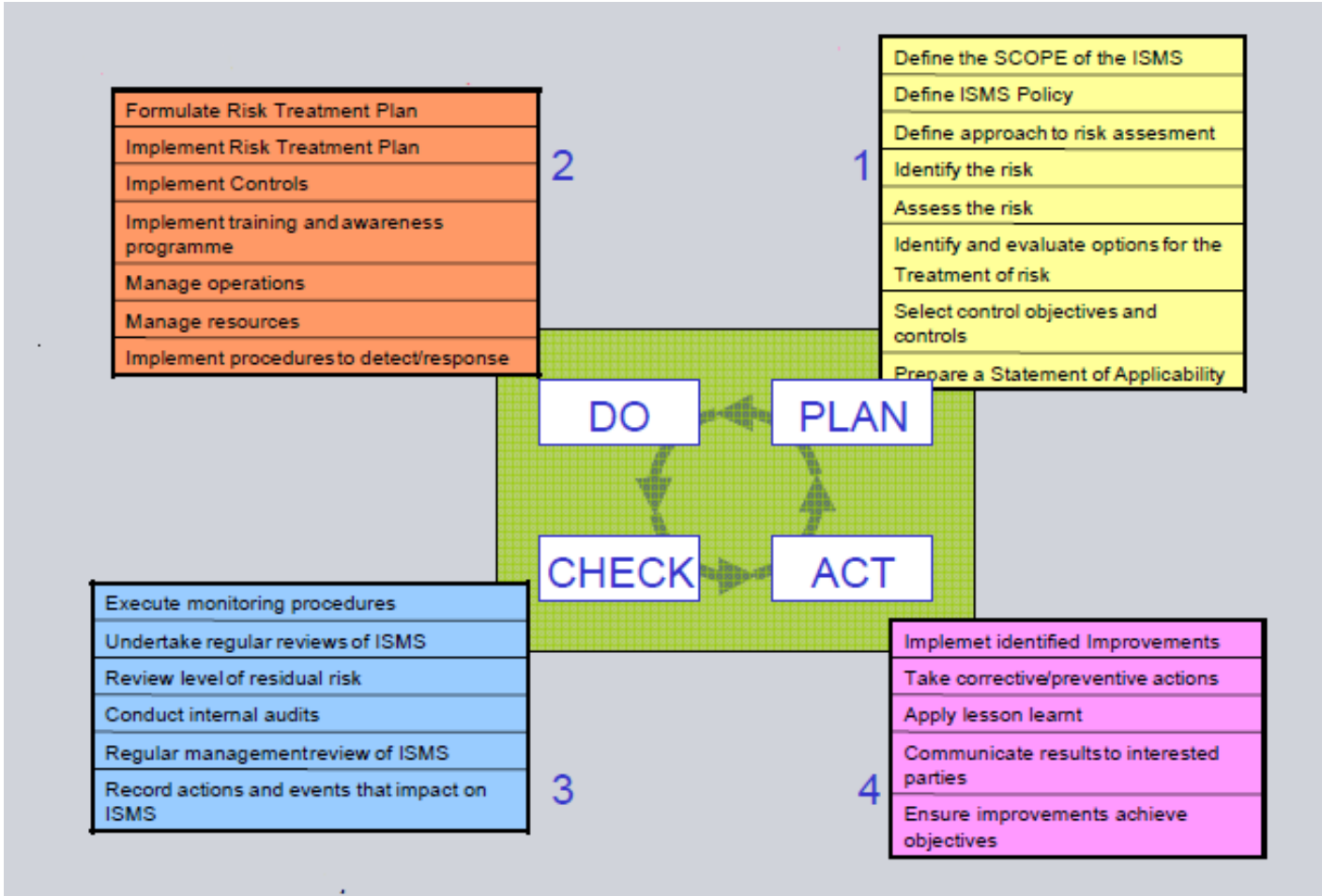
But the problem is to determine how much is too much, so that we can implement appropriate security measures to build adequate confidence and trust

Management Systems

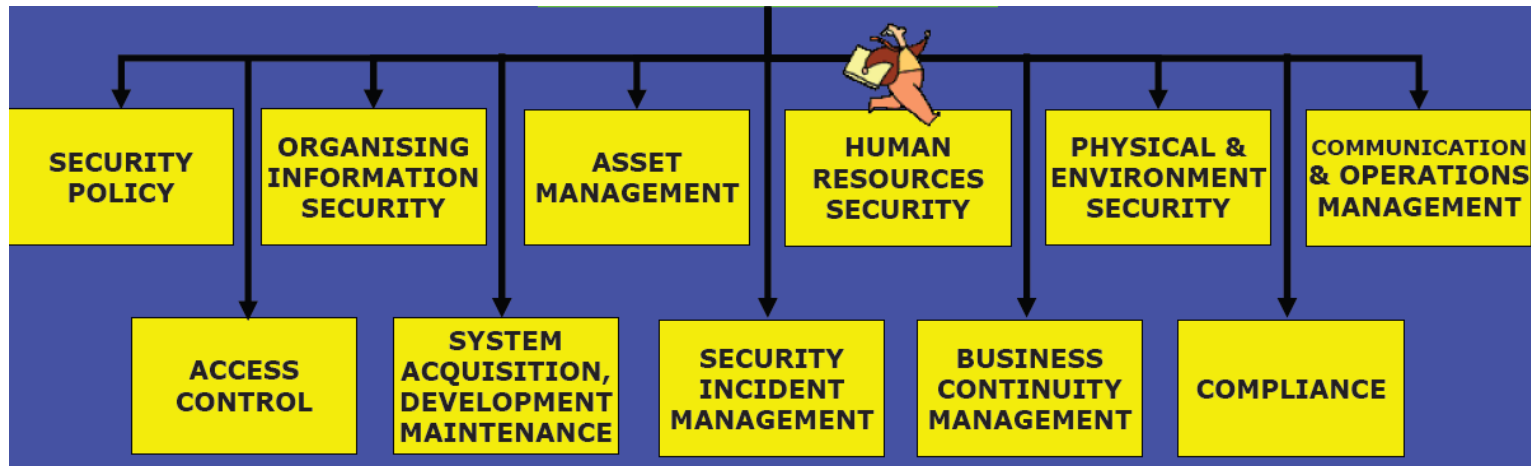


Management systems provide assurance through a discipline of compliance

ISMS Reference framework



ISMS –Security Domains



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.

Steps for successful implementation



Can we order the steps right?

- Monitor implementation
- Define a method of risk assessment
- Determine the scope of ISMS
- Obtain management support
- Identify controls and objectives applicable to risks
- Purchase a copy of the ISO standards
- Identify risks
- Train and Implement
- Setup policy & procedures

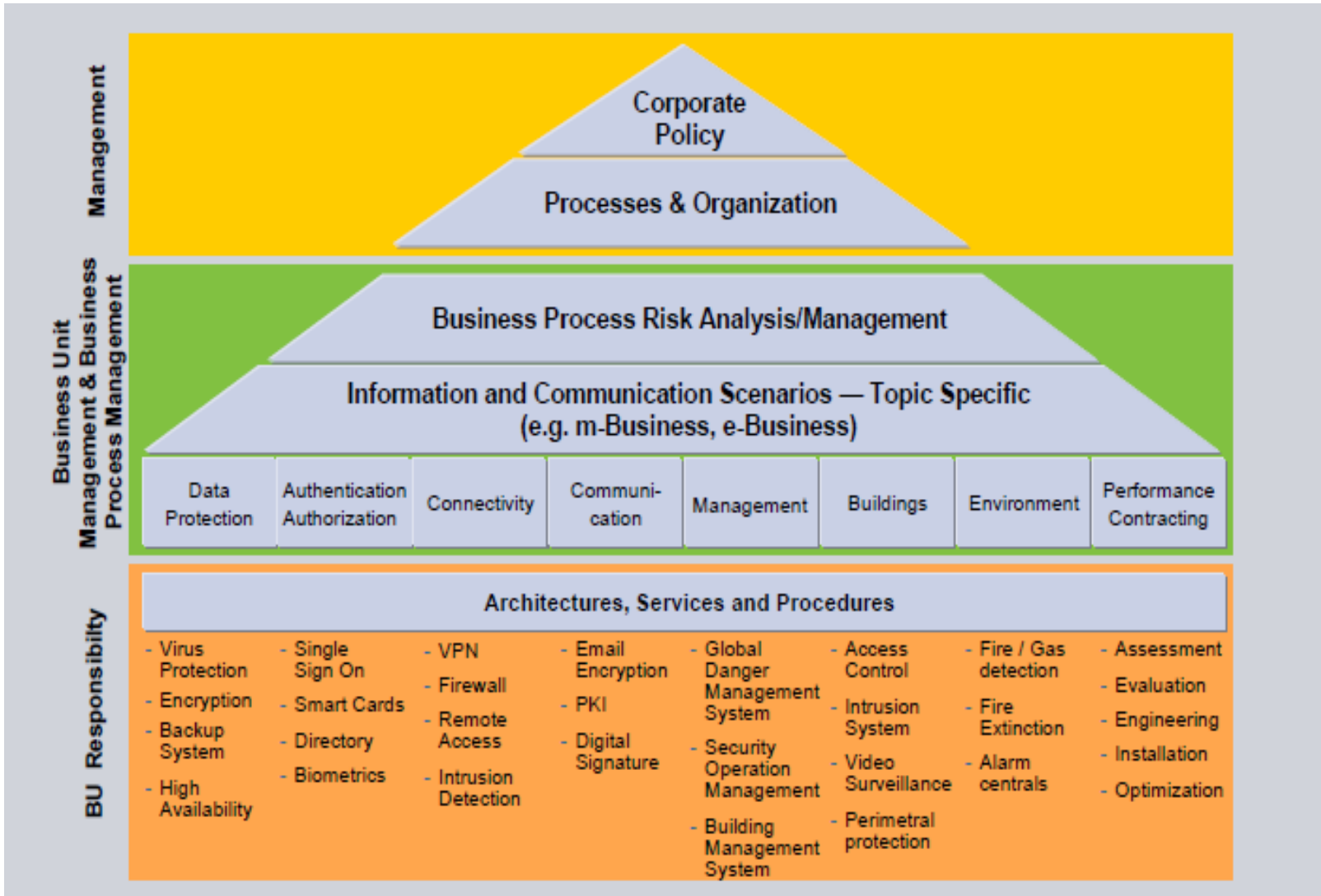
Steps for successful implementation



Is the order right?

1. Purchase a copy of the ISO / IEC standards
2. Obtain management support
3. Determine the scope of ISMS
4. Define a method of risk assessment
5. Identify risks
6. Identify controls and objectives applicable to risks
7. Setup policy & procedures
8. Train and Implement
9. Monitor implementation

Security Framework- Example



Some interesting quotes

- ❑ Management of information security is a much deeper and more political problem than is usually realized
- ❑ The only true secure system is the one that is powered off, cast in a block of concrete sealed in a lead-lined room with armed guards
- ❑ A common view is information security comes down to technical measures. Information insecurity is at least as much due to perverse incentives.

