QMI™

Management Systems Registration

UMB

Information Security Management Systems

Presented by
Eng. Mohamad Fawaz
Managing Partner QMI-UMB

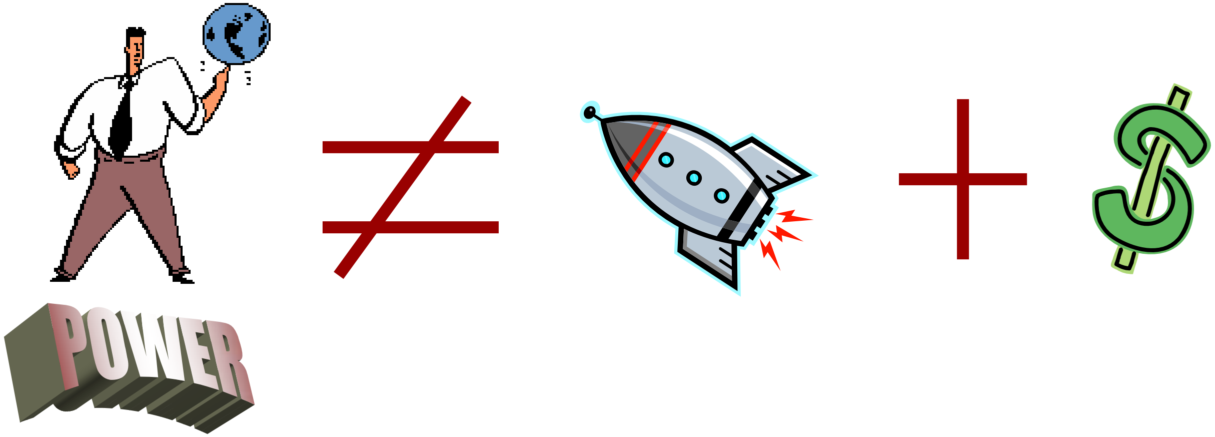
Outline

- Introduction
- Information types
- Information Security
- Information Security Management System (ISMS)
- ISMS Standards
- PDCA cycle for ISMS
- Certification of ISMS

Introduction

- The Paradigm shift from Industrial to Knowledge era has changed our perceptions of value and influence

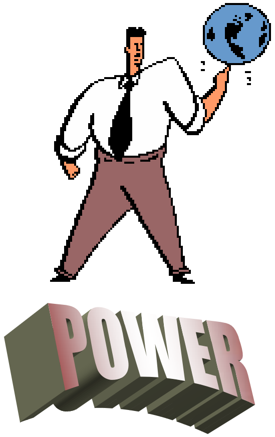
- Power is no longer measured by the size of financial wealth or abundance of other resources



Introduction

- The Paradigm shift from Industrial to Knowledge era has changed our perceptions of value and influence

- Power is no longer measured by the size of financial wealth or abundance of other resources



= ℹ

- Information is the most important asset

Information types

Information can be:

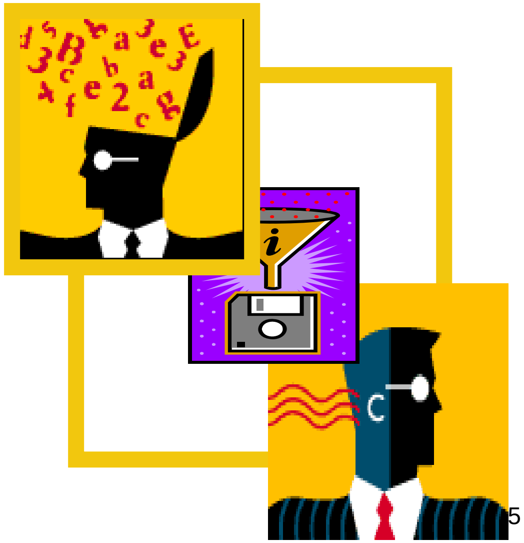
- created
- stored
- destroyed
- Used
- Transmitted

Character of information

- Financial
- Strategic
- Operational
- Person dependent
- …

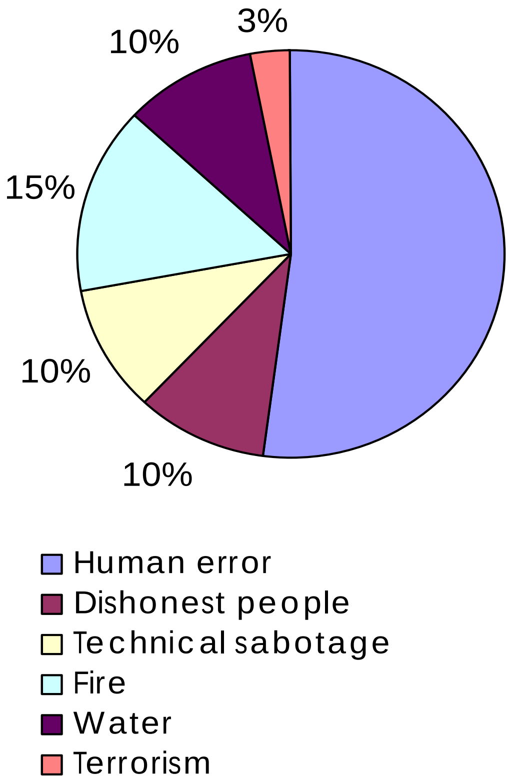
Information format

- Paper
- Databases
- Disk(ette)s
- CD-ROMs
- Tapes
- (Design) drawings
- Films
- Conversations
- …

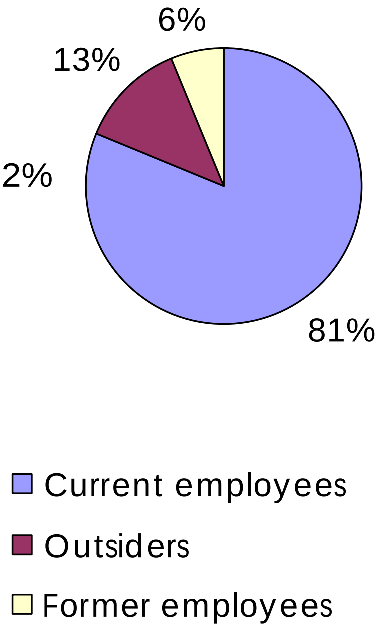


Causes of Information Damage

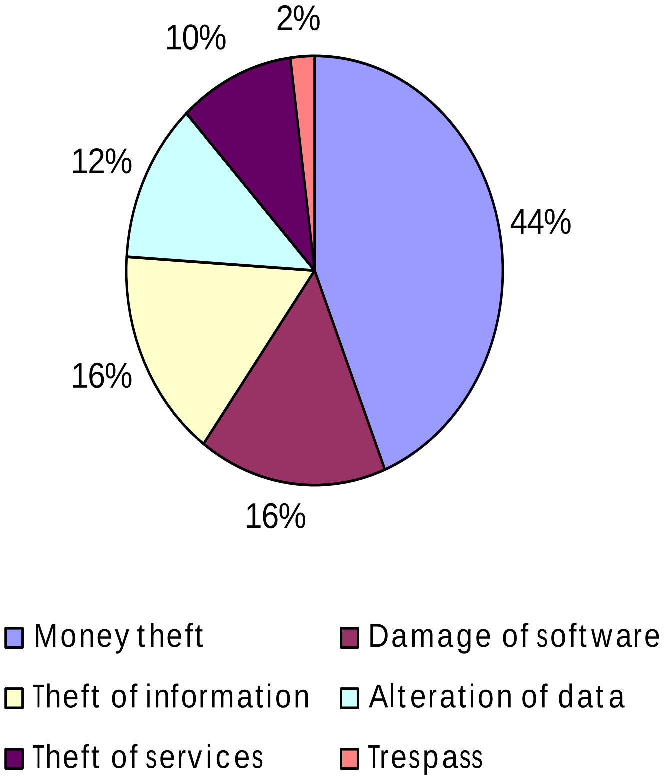
Common Causes of damage



Who causes damage



Types of computer crime



Information Security

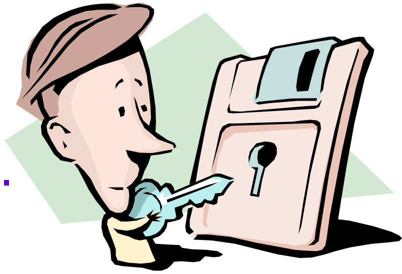
- High dependence on information as a contributing factor of success or failure, created the need for information security and control
- Information security definition:

  "preservation of confidentiality, integrity and availability of information and information systems"

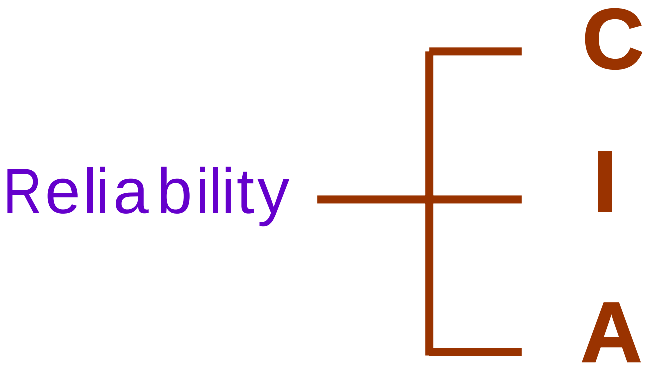
- The objective of information security is to ensure the continuity of business management and to reduce interruptions of business by preventing and minimizing the consequences of security incidents. Information security relates to all controls aimed at protecting the availability, integrity and confidentiality of information.

Importance of Information Security

- Information security is essential for an enormous range of organizations, not only because of their own dependence on the information, but also because of the trust that stakeholders place in these organizations. After all, more and more information is being exchanged.
- Almost every organization (companies, government bodies and non-profit organizations) has become more and more dependent on computers over the last decades. In addition, the use of computer networks has increased, not only within organizations, but also between organizations and the outside world.
- As a result of increasing and more vulnerable to, for example, acts of God, technical faults and human error, in addition, the much-cited computer viruses and hackers pose new, contemporary threats. These trends mean that organizations are having to devote more and more attention to information security.



Information Security Components



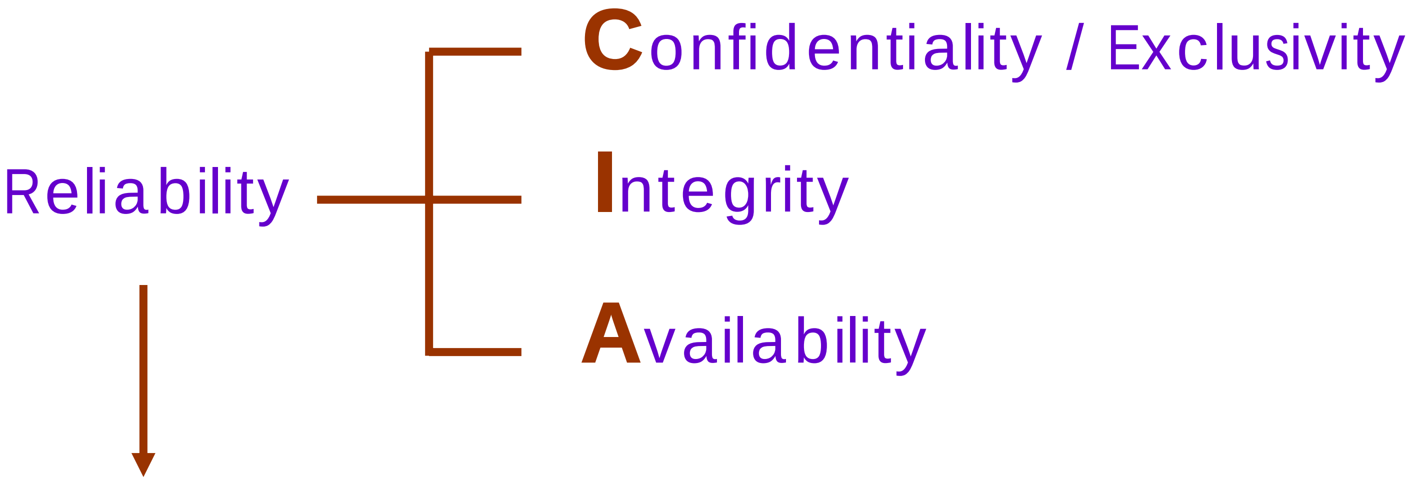
Reliability

C

I

A

Information Security Components



Reliability

Confidentiality / Exclusivity

Integrity

Availability

The degree to which the organization can depend upon an information system for its provision of information

Information Security

Confidentiality: exclusivity

- Relates to the limitation of authority and opportunities for access, alteration, printing or copying of information by a defined group of authorized persons
  - Other issues include barriers and permissions

Information Security

Integrity: information accuracy and completeness

- Defined as the “accuracy” and “completeness” of information
- Implies that the information reflects the described reality
- As well as accuracy and completeness, other issues are currency, authenticity and consistency.

Information Security

Availability : the smooth running of information delivery

- Refers to the unimpeded progress (continuity) of the provision of information
- other aspects include adaptability, business security, restart-ability, maintainability, durability, reproducibility, robustness and replicability
- A Yankee Group report estimated that downtime caused by security incidents cost as much as $4,500,000 per hour for brokerages and $2,600,000 for banking firms.

Information Security Management System (ISMS)

Definition:

- that part of the overall management system, based on a business risk approach, to
  - establish,
  - implement,
  - operate,
  - monitor,
  - maintain and
  - Improve information security

- The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources

ISMS Standards : BS7799-2/ISO27001 and ISO17799

BS7799-2/ISO27001

- formal standard
- certification possible
- requirements for a management system
- requirements for controls (if applicable)

⟺

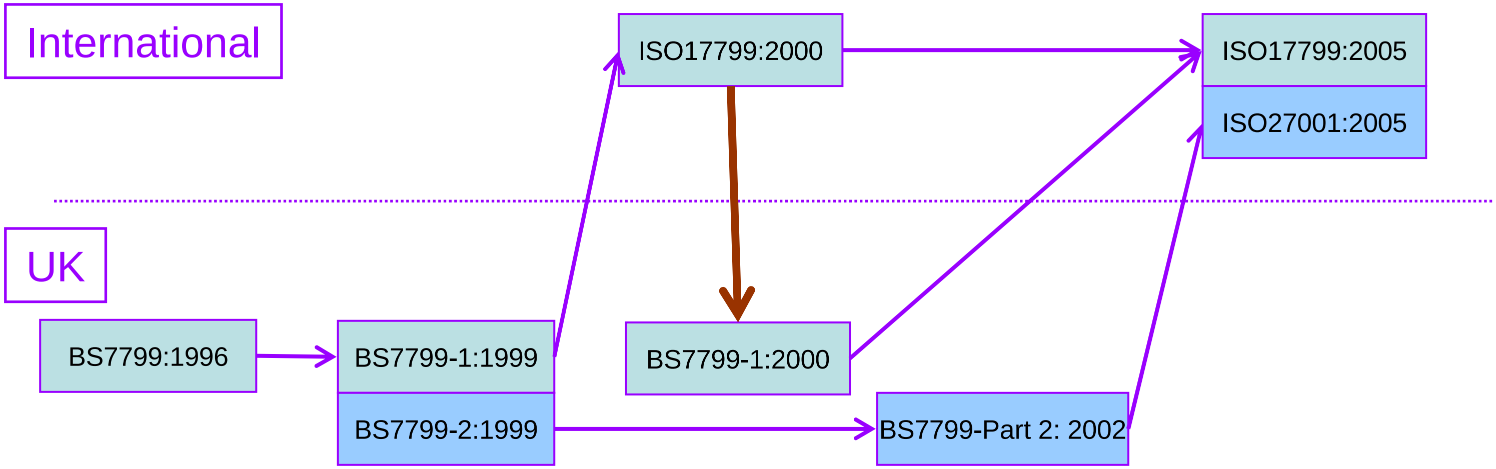
ISO 17799:2000/2005

- code of practice (set of best practices)
- implementation advice and guidance

What are BS7799-2 and ISO17799 not

- limited to information technology
- a security checklist
- an insurance policy against security breaches
- an audit method
- a risk analysis method

History of ISMS Standards



International

UK

ISO17799:2000

ISO17799:2005

ISO27001:2005

BS7799:1996

BS7799-1:1999

BS7799-2:1999

BS7799-1:2000

BS7799-Part 2: 2002

→ = copy/translation

→ = revision

Structure of BS 7799-2 / ISO 27001

- Introduction, Scope, References and Terms and definitions

- Requirements for an ISMS
  - General requirements
  - Management responsibility
  - Internal ISMS audits (in ISO27001 in a separate chapter!)
  - Management review of the ISMS
  - ISMS improvement

- Control objectives and controls in Annex A, normative

Structure of BS 7799-2 / ISO 27001

BS7799-2, Annex A

- 10 Areas of concern
- 36 Control objectives
- 127 Controls

ISO27001:2005, Annex A

- 11 Areas of concern
- 40 Control objectives
- 136 Controls

Important Areas of Concern

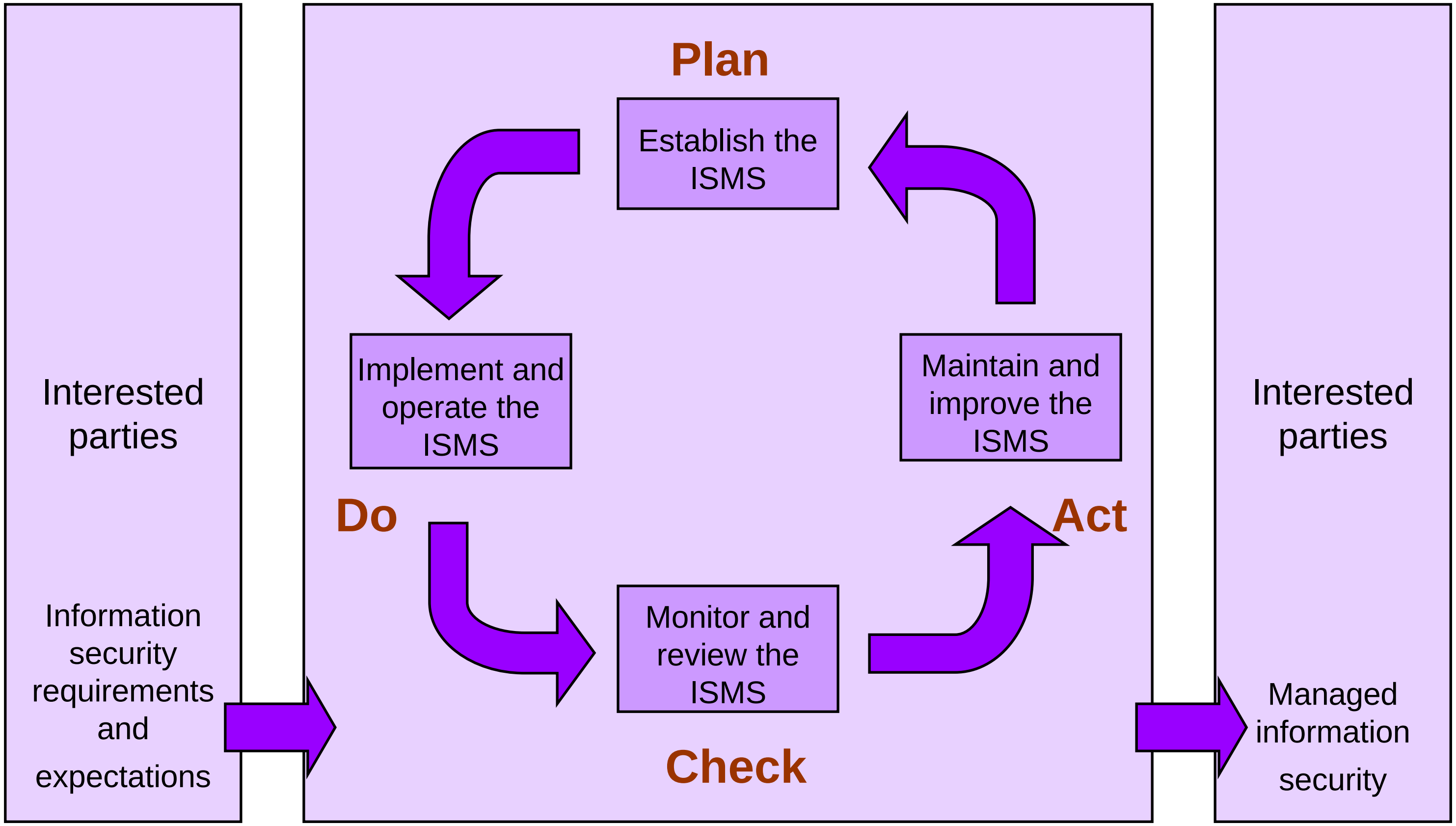
BS7799-2

1. Security policy (3)
2. Organizational security(4)
3. Asset classification and control (5)
4. Personnel security (6)
5. Physical and environmental security (7)
6. Communications and operations management(8)
7. Access control (9)
8. System development and maintenance (10)
9. Business continuity management (11)
10. Compliance (12)

ISO27001

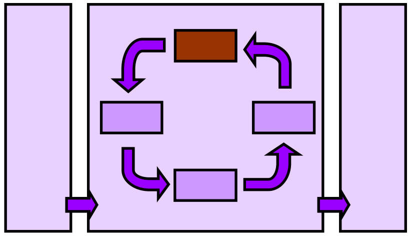
1. Security policy (5)
2. Organization of information security (6)
3. Asset management(7)
4. Human resources security (8)
5. Physical and environmental security (9)
6. Communications and operations management (10)
7. Access control (11)
8. Information systems acquisition, development and maintenance (12)
9. Information security incident management (13)
10. Business continuity (14) management
11. Compliance (15)

Plan Do Check Act Cycle (PDCA)



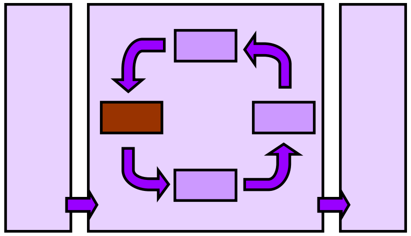
Interested parties
Information security requirements and expectations
Plan
Establish the ISMS
Implement and operate the ISMS
Maintain and improve the ISMS
Do
Act
Monitor and review the ISMS
Check
Interested parties
Managed information security

PDCA



Establish the ISMS

- Define the scope of the ISMS
- Define an ISMS policy
- Define a systematic approach to risk management
- Identify the risks
- Assess the risks
- Identify and evaluate options for the treatment of risks
- Select control objectives and controls for the treatment
- of risks
- Prepare a Statement of Applicability
- Obtain management approval for residual risks and authorization to implement and operate the ISMS

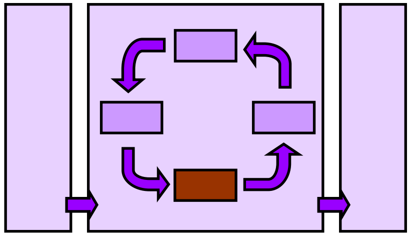


PDCA

Implement and operate the ISMS

- Formulate a risk treatment plan
- Implement the risk treatment plan
- Implement the controls selected
- Implement training and awareness programs
- Manage operations
- Manage resources
- Implement procedures and controls to detect and response to security incidents

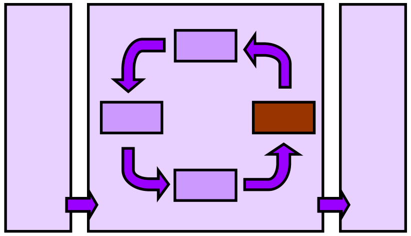
PDCA



Monitor and review the ISMS

- Execute monitoring procedures
- Undertake regular reviews
- Review level of residual risk
- Conduct internal audits
- Undertake a management review
- Record actions and events

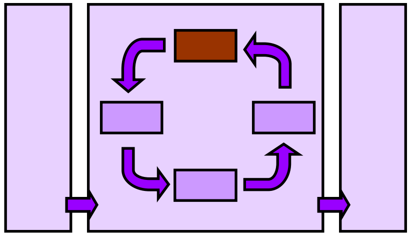
PDCA



Maintain and improve the ISMS

- Implement the identified improvements
- Take appropriate corrective and preventive actions
- Communicate results
- Ensure effectiveness

PDCA



Establish the ISMS

- Define the scope of the ISMS
- Define an ISMS policy
- Define a systematic approach to risk management
- Identify the risks
- Assess the risks
- Identify and evaluate options for the treatment of risks
- Select control objectives and controls for the treatment
- of risks
- Prepare a Statement of Applicability
- Obtain management approval for residual risks and authorization to implement and operate the ISMS

Certification of ISMS

Certification Process

Normally spanning 1-3 months, includes 3 phases:

Phase 1

- audit of the risk assessment process, selection of controls and creation of the Statement of Applicability
- creation of the audit plan for Phases 2 and 3, and the surveillance audit

Phase 2

- audit of the ISMS documentation
- update of the audit plan for Phase 3 (if necessary)

Phase 3

a. audit of the implementation of the ISMS
   - is the PDCA loop effective?
   - are the selected controls effectively implemented?

Certification of ISMS (cont'd)

- The certificate is valid for a period of three years
- The certificate refers to the Statement of Applicability

- Surveillance audits
  - once a year
  - once every 6 months

      - coverage of all processes and controls over the three year period

Thank you!

Questions?