سمینار آموزشی سیستم مدیریت امنیت اطلاعات بر پایه سیاستهای استانداردهای BS7799 & BS15000

DNV
ISERC

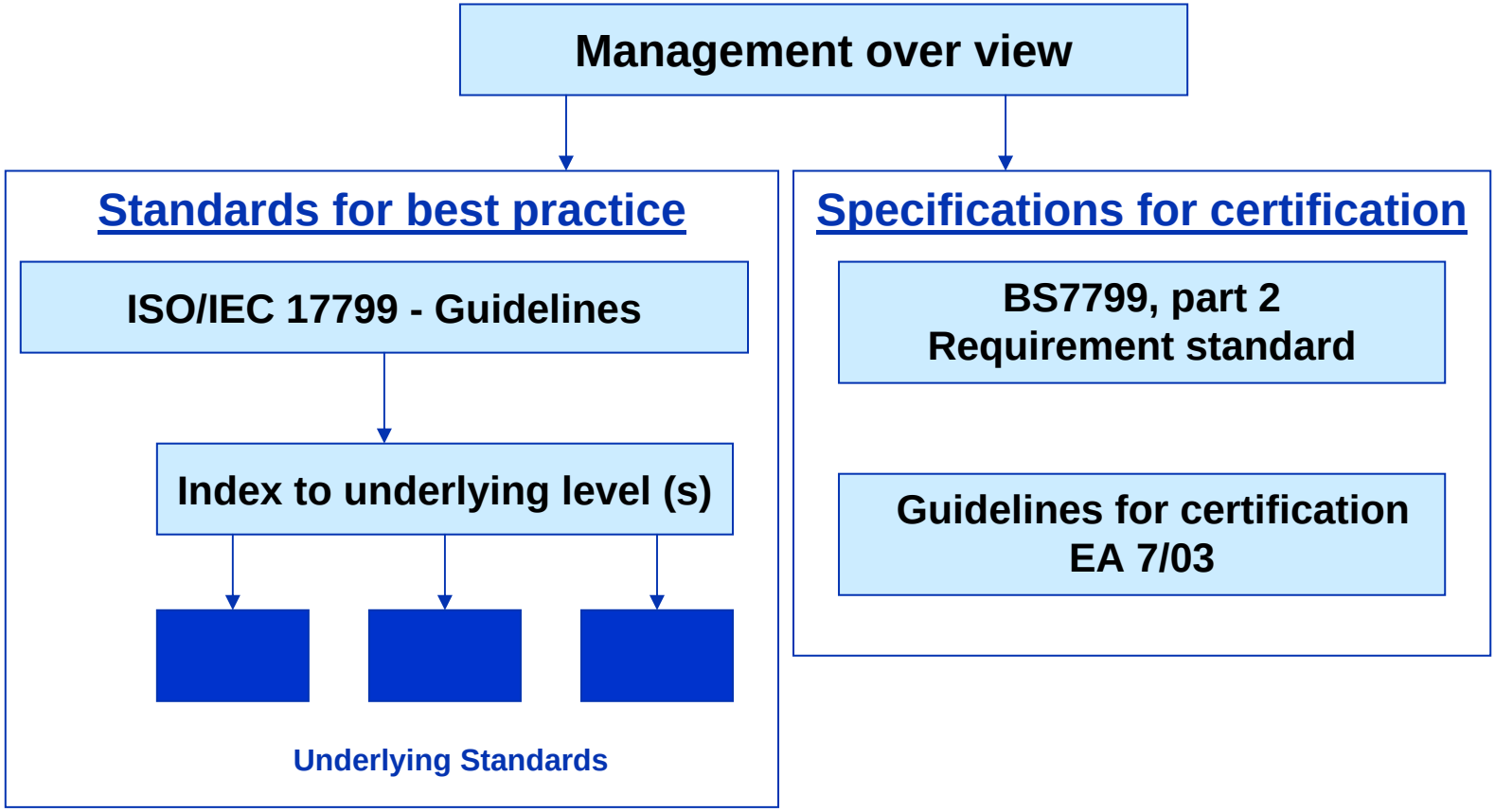
سمینار آموزشی دوم

Part Two

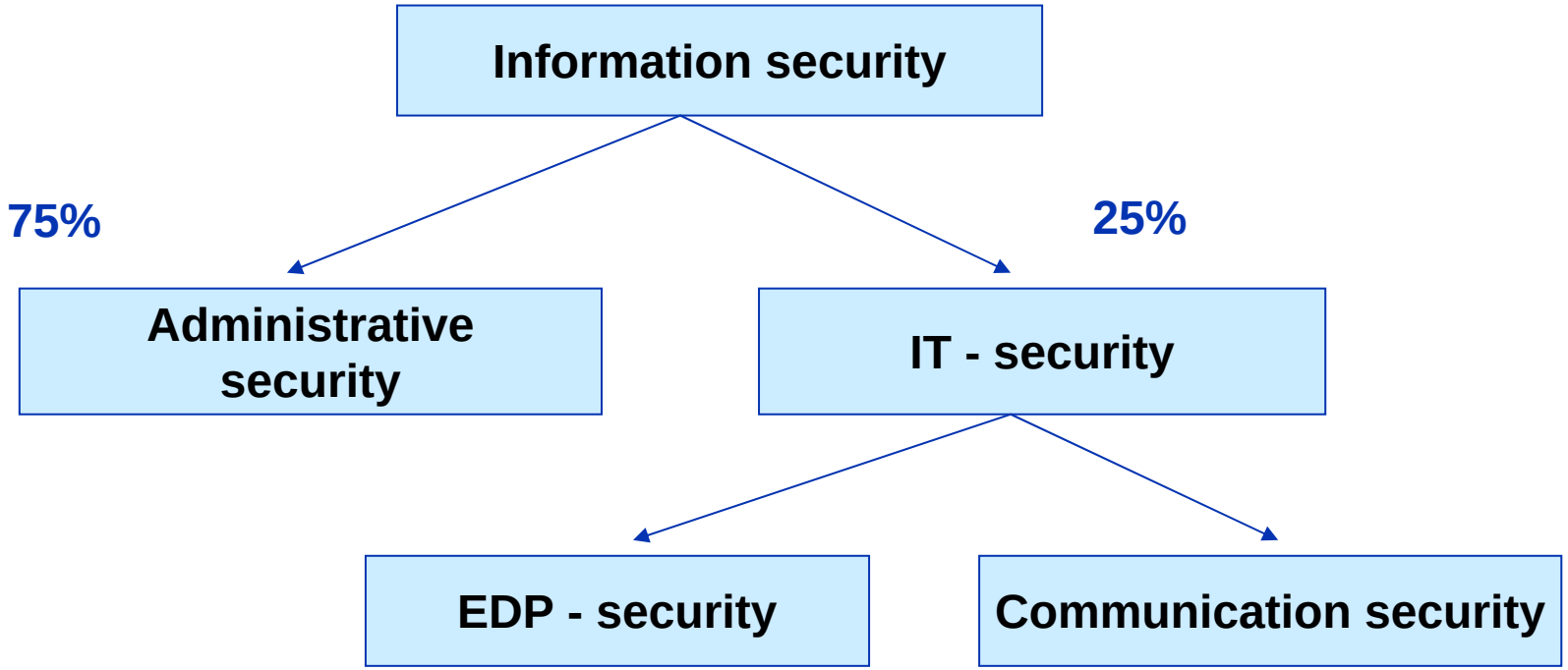
Implementation of BS7799/ISO17799 Controls

Houman Sadeghi Kaji
Spread Spectrum Communication System PhD. ,
Cisco Certified Network Professional Security Specialist
BS7799 LA
info@iserc.info

Structure


Management over view
Standards for best practice
ISO/IEC 17799 - Guidelines
Index to underlying level (s)
Underlying Standards
Specifications for certification
BS7799, part 2
Requirement standard
Guidelines for certification
EA 7/03

Information Security - Structure



The ISO 17799 Way

Safeguarding the confidentiality, integrity, and availability of written, spoken, and computer information

ISO 17799 Is

- **An internationally recognized structured methodology dedicated to information security**
- **A defined process to evaluate, implement, maintain, and manage information security**
- **A comprehensive set of controls comprised of best practices in information security**
- **Developed by industry for industry**

DET NORSKE VERITAS

MANAGEMENT SYSTEM CERTIFICATE

InfoFarm Co., Ltd.

BS 7799-1:2002

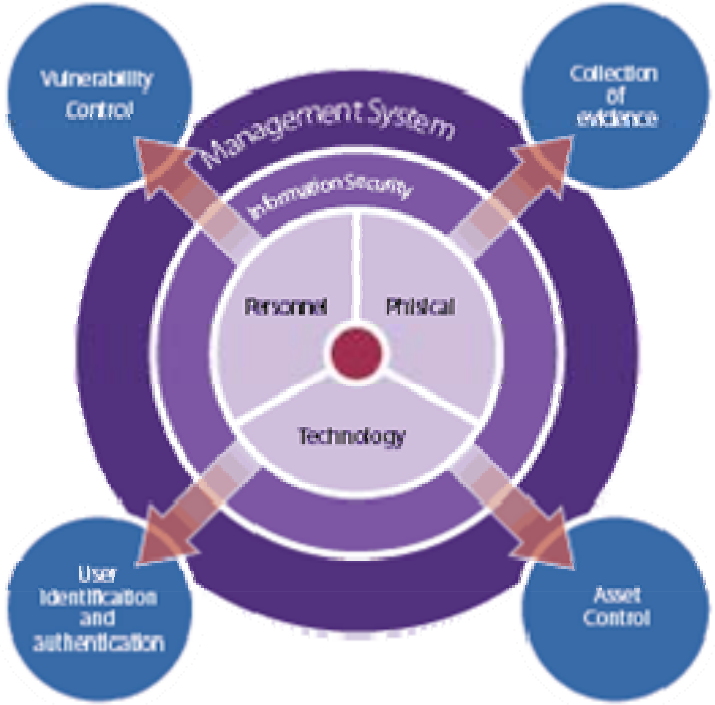
Network Service (ISP, Housing, Hosting),
Design and Construction of Network,
Development of Internet Website,
All in accordance with latest version of statement of applicability

ISO 17799 Is Not

- **A technical standard**
- **Product or technology driven**
- **An equipment evaluation methodology such as the Common Criteria/ISO 15408**
  - **But may require utilization of a Common Criteria Equipment Assurance Level (EAL)**
- **Related to the "Generally Accepted System Security Principles," or GASSP**
  - **But may incorporate GASSP guidelines**
- **Related to the five-part "Guidelines for the Management of IT Security," or GMITS/ISO TR 13335**
  - **But may implement GMITS concepts**

Holistic Approach

- **ISO 17799 defines best practices for information security management**
- **A management system should balance physical, technical, procedural, and personnel security**
- **Without a formal Information Security Management System, such as a BS 7799-2 based system, there is greater risk of your security being breached**
- **Information security is a management process, not a technological process**



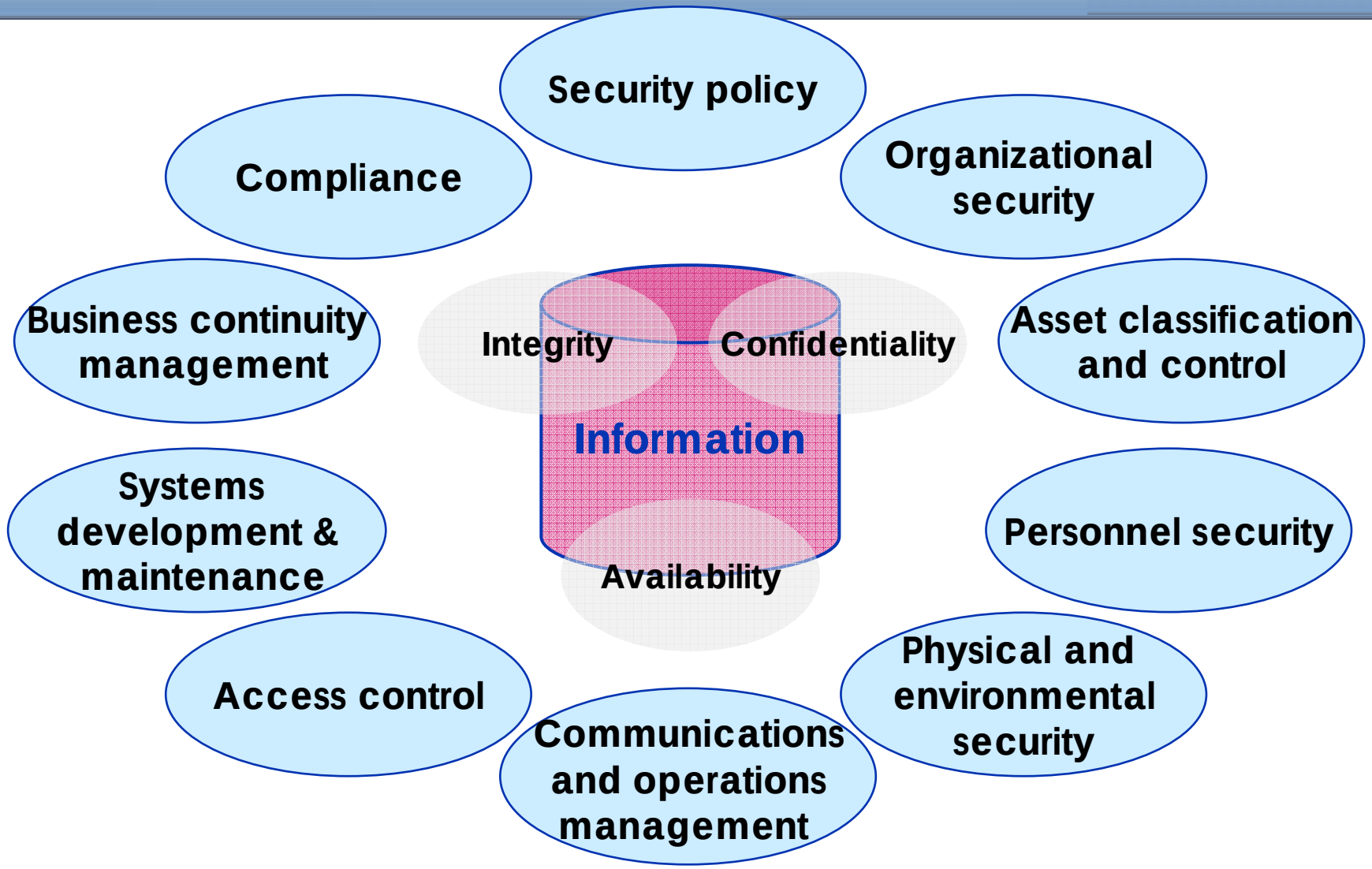
ISO 17799 Standards

- ISO/IEC 17799:2000
  Code of Practice for Information Security Management

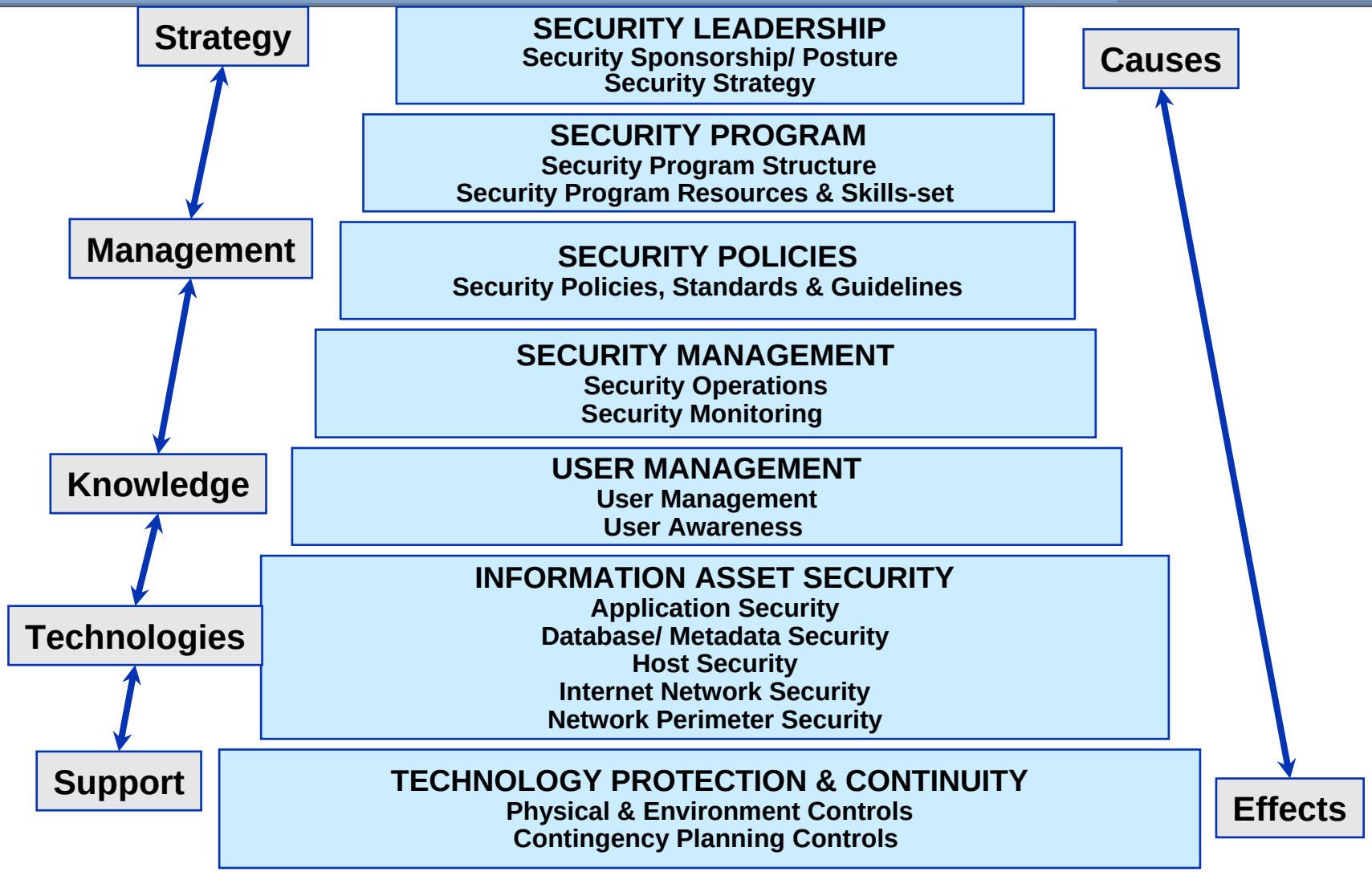
- BS 7799-2:2002

  Specification for Information Security Management Systems

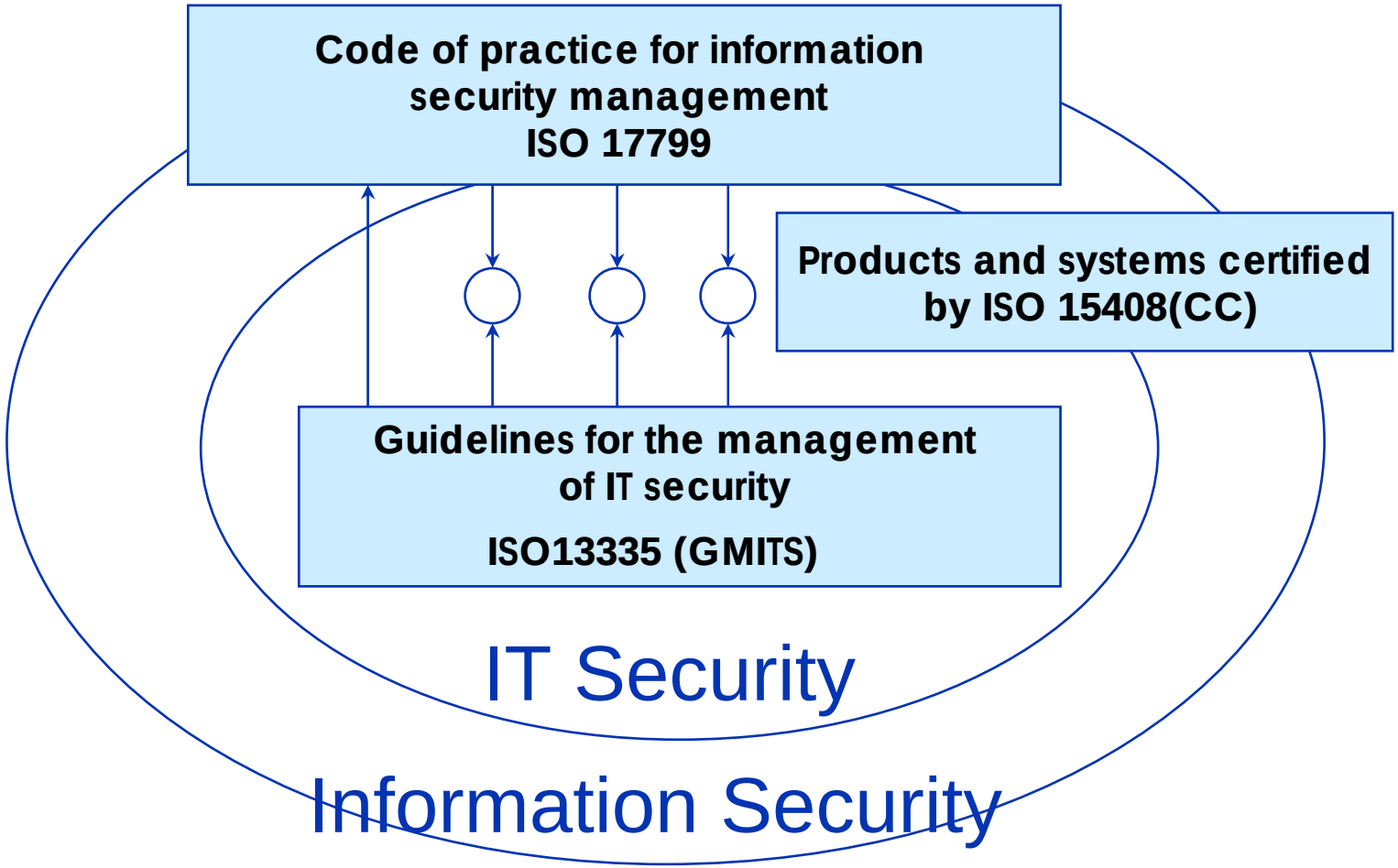
The 10 Sections of ISO 17799



The 10 Sections of ISO 17799 (continued)



Complementarily with Other ISO Standards



Specifications with Guidance

1.Scope

2.Normative references

3.Terms and definitions

4.Information security management system requirements

5.Management responsibility

6.Management review of the ISMS

7.ISMS improvement

Annex A - (Normative) Control objectives and control

Annex B - (Informative) Guidance on use of the standard

Annex C - (Informative) Correspondence between

Code of Practice

- **Scope**

  - **This part provides recommendations for information**
  - **Security management for use by those who are**
  - **Responsible for initiating, implementing or maintaining**
  - **Security in their organization.**
  - **It is intended to provide a common basis for developing**
  - **Organizational security standards and effective security**
  - **Management practice and to provide confidence in**
  - **Interorganizational dealings**

Code of Practice

3.Security policy

4.Organisational security

5.Asset classification and control

6.Personnel security

7.Physical and environmental security

8.Communications and operations management

9.Access control

10.Systems development and maintenance

11.Business continuity management

12.compliance

Management Responsibility

- **Management Commitment**
  - Provide evidence of its commitment
  - Decide the level of acceptable
  - Conduct management reviews
- **Resource management**
  - Provide necessary resources
  - Ensure that personnel are competent

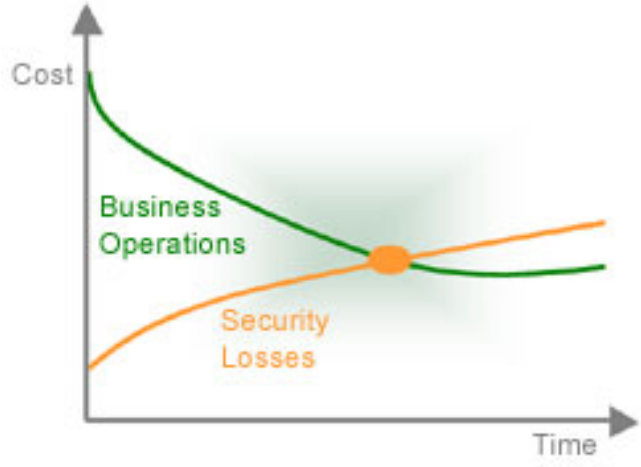
Annex a – Control Objectives and Controls

- **BS 7799-2 ISO 17799** contains:
  - 10 control clauses, 36 control objectives, and 127 controls
- "Not all of the guidance and controls in this code of practice may be applicable. Furthermore, additional controls not included in this document may be required."
- "They are either based on essential legislative requirements or considered to be common best practice for information security."
- "…guiding principles providing a good starting point for implementing information security."

Main Information Security Issues

- Only 40% of organizations are confident they would detect a systems attack
  - A.9.7 Monitoring system access and use

  Objective: To detect unauthorized activities
  - A.9.7.1 Event logging
  - A.9.7.2 Monitoring system use
  - A.9.7.3 Clock synchronization



Main Information Security Issues

- 40% of organizations do not investigate information security incidents
  - A.6.3 Responding to security incidents and malfunctions

  Objective: To minimize the damage from incidents or malfunctions and to monitor and learn from such incidents
    - A.6.3.1 Reporting security incidents
    - A.6.3.4 Learning from incidents

Main Information Security Issues

- Critical business systems are increasingly interrupted - over 75% of organizations experienced unexpected unavailability
  - A.8.2 System planning and acceptance

  Objective: To minimize the risk of systems failures
    - A.8.2.1 Capacity planning
    - A.8.2.2 System acceptance

Main Information Security Issues

- Business continuity plans exist in only 53% of organizations
  - A.11 Business continuity management

  Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
    - A.11.1.1 Business continuity management process
    - A.11.1.3 Writing and implementing continuity plans
    - A.11.1.5 Testing, maintaining, and re-assessing business continuity plans

Main Information Security Issues

- Only 41% of organizations are concerned about internal attacks on systems, despite overwhelming evidence of the high number of attacks from within organizations
  - A.6 Personnel Security

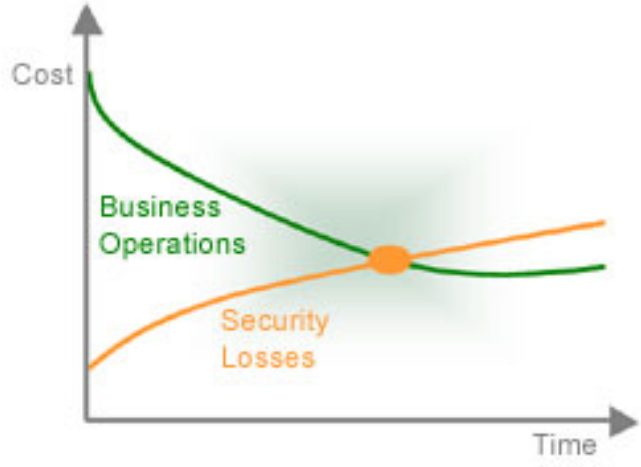
  Objective: To reduce the risks of human error, theft, fraud, or misuse of facilities
  - A.7 Physical and environmental security

  Objective: To prevent unauthorized access, damage, and interference to business premises and information

Main Information Security Issues

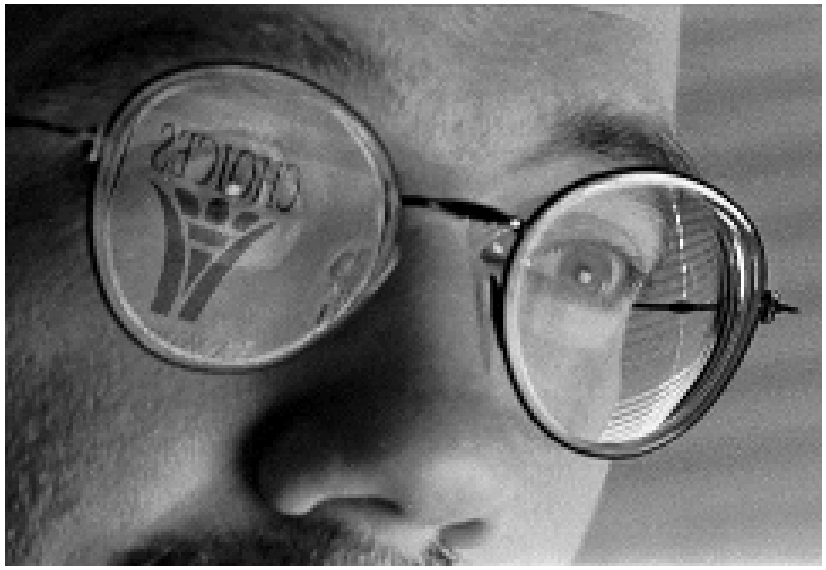
- Less than 50% of organizations have information security training and awareness programs
  - A.6.2 User Training

  Objective: To ensure that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work



Establishing a Management Framework

- **Define Scope of the ISMS**
- **Define Policy**
- **Define Approach to Risk Assessment**
- **Identify the Risks**
- **Assess the Risks**
- **Identify options for treatment of risks**
- **Select control Objectives and Controls**
- **Statements of applicability**
- **Obtain management approval**



To be REVIEWED at APPROPRIATE INTERVALS!

4.2. a) The Scope of the ISMS

- Characteristics of the organization
- Business
- Location
- Assets
- Technology

FROM Business's NEEDS !

NOT ONLY IT !

4.2.1 c-d) Risk Assessment

- **Define systematic approach to risk assessment**
  - **Suitable Method**
  - **Criteria for Accepting Risks**
  - **Level of Accepting Risks**

- **Identify risks**
  - **Threats to Assets**
  - **Vulnerabilities of Assets**
  - **Impacts on the Assets**

FROM THE NEEDS OF THE BUSINESS !

NOT ONLY IT !

4.2.1 e) Assess the Risks

- **Assess harm to business caused by loss of an assets' :**
  - **confidentiality**
  - **integrity**
  - **availability**
- **Assess the Probability and Impact of a Failure**
- **Estimate the Levels of Risks**
- **Determine whether the risk is acceptable or not**

FROM THE NEEDS OF THE BUSINESS !

NOT ONLY IT !

3) SECURITY POLICY

- Provide **Direction** and
- **Support** for information security

3.1) Information Security Policy

Objective: To provide management direction and support for information security

Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization

Based on the Risk Analysis !

3.1.1) Information Security Policy Document

- **Definition of information security**
- **A statement of management intent**
- **Security policy, principles, standard and compliance requirements of particular importance**
- **Definition of responsibility for information security**
- **Reference to documentation which may support the policy**

Based on the Risk Analysis !

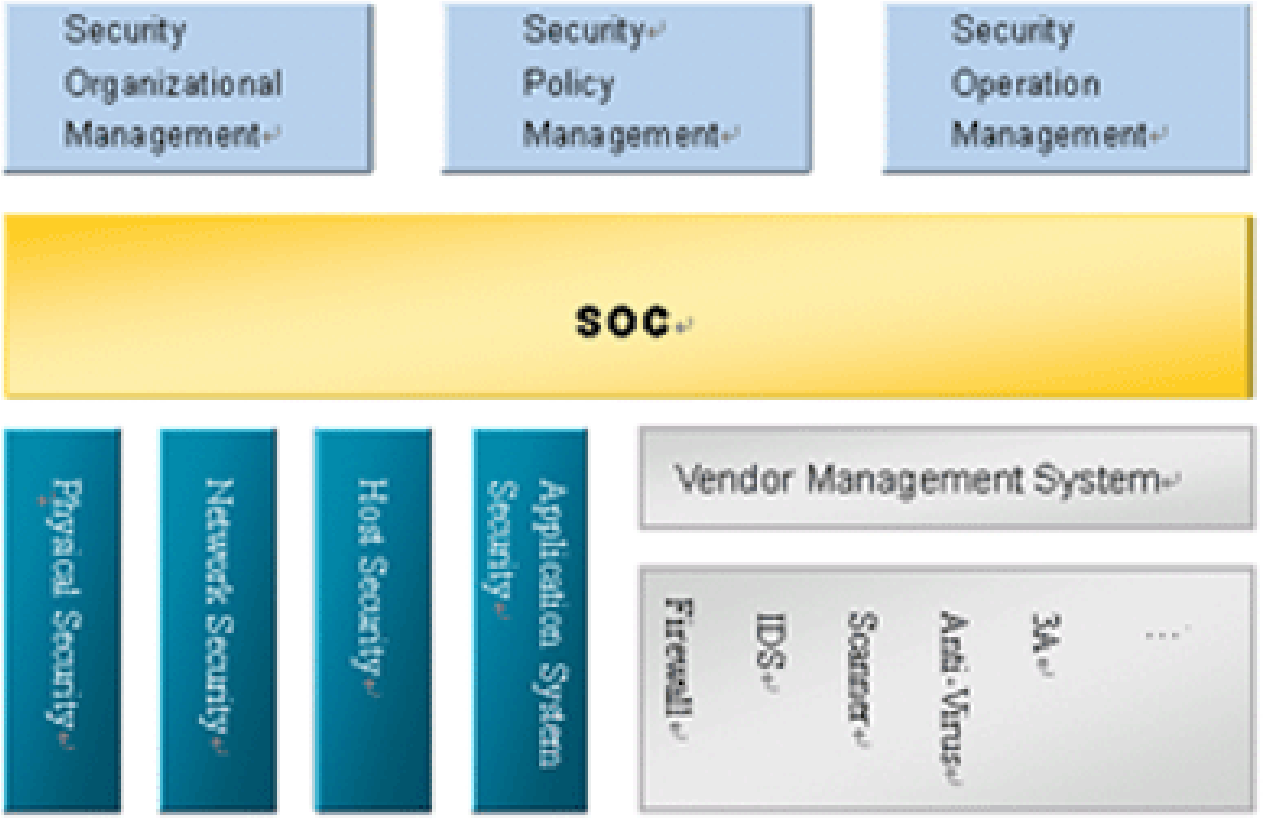
3.1.2) Review and Evaluation

- **Effectiveness demonstrated by the recorded incident**
- **Cost and impact of controls on business efficiency**
- **Effects of changes to technology**

Based on the Risk Analysis !

12.2) Review of Security Policy and Technical Compliance

Objective: To ensure compliance of systems with organization security policies and standard



12.2.1) Compliance with security Policy

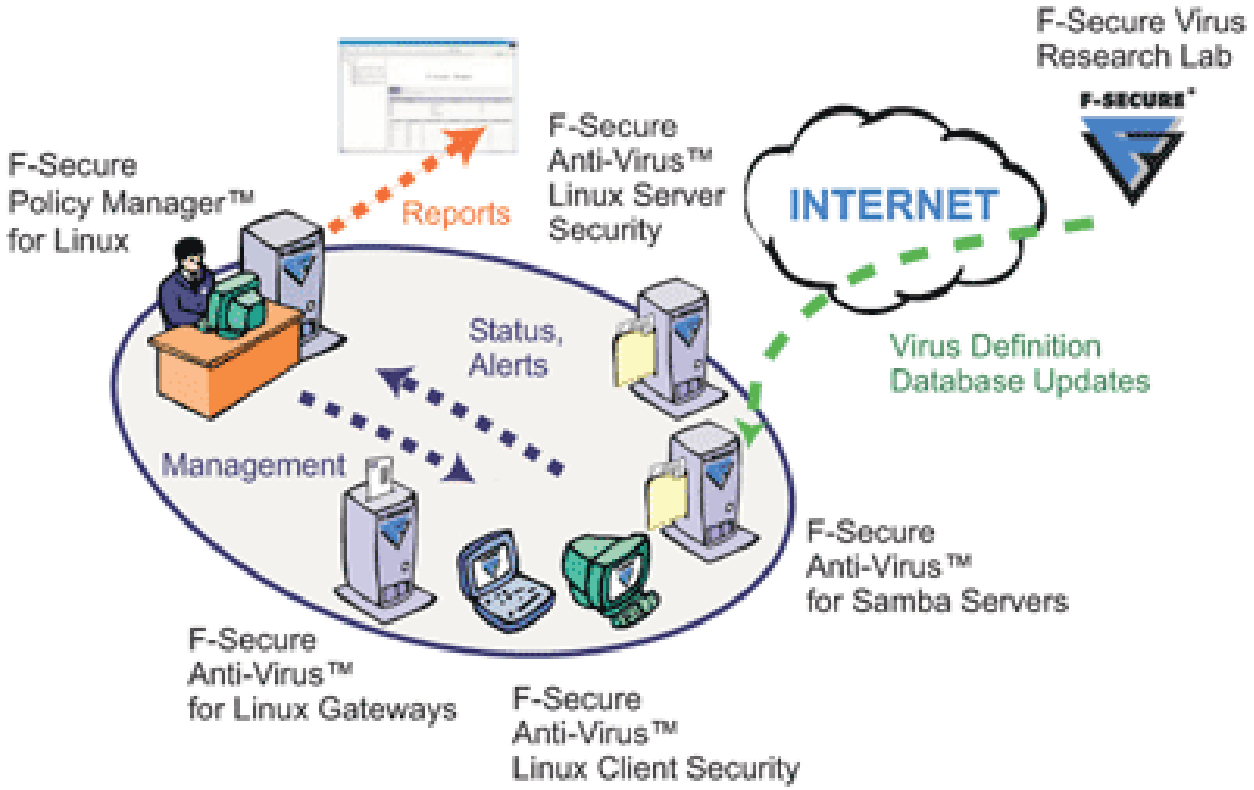
Managers should ensure that a;ll security procedures whithin their area of responsibility are carried out correctly.

Regular Review :

- **Information systems**
- **Systems Providers**
- **Owner of Information and Information Assets**
- **Management**

12.2.2) Technical compliance checking

Information systems shall be regularly checked for compliance with security implementation standards



4) ORGANISATIONAL SECURITY

4.1 INFORMATION SECURITY INFRASTRUCTURE

Objective: To manage information security within the organization .

A management framework should be established to initiate an implementation of information security within the organizatio

Suitable management for a with management leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization…

4) ORGANISATIONAL SECURITY

4.1.1 Management Information Security Forum

Information security is a business responsibility shared by all members of the management team .

- **Reviewing and approving information security policy and overall responsibilities**
- **Reviewing and monitoring security incidents**
- **Monitoring significant changes in the exposure of information assets to major threats**
- **Approving major initiatives to enhance information security**

One manager should be responsible for all security related activities

4) ORGANISATIONAL SECURITY

4.1.2 Information security co-ordination

cross-functional forum (larger organization)

- **Specific roles and responsibilities across the organization**
- **Methodologies and processes; e.g. risk assessment , security classification system**
- **Security awareness programs**
- **Security – part of the information planning process**
- **Review information security incidents**

4) ORGANISATIONAL SECURITY

4.2 SECURITY OF THIRD PARTY ACCESS

Objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties.

- **Controlled**
- **Appropriate risk assessment – controls should be agreed and defined in a contract with the third party**

4) ORGANISATIONAL SECURITY

4.2.1 Identification of risks from third party access

- **Type of access (4.2.1.1)**

  - physical and/or logical
- **Reasons for access (4.2.1.2)**

  - support staff and/or trading partners
- **On-site contractors (4.2.1.3)**

  - hardware and software maintenance and support staff

  - cleaning, catering, security guards etc

  - student placement and other casual short term appointments

  - consultants

4) ORGANISATIONAL SECURITY

4.2.2 Security requirements in third party contracts

- Formal contract
- Security requirements
- Responsibilities
- Indemnity of the supplier
- The right to audit
- Escalation process

4) ORGANISATIONAL SECURITY

4.3 OUTSOURCING

Objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organization .

Outsourcing arrangements should address the risks, security controls and procedures for information systems, network and/or desk top environments in the contract between the parties .

4) ORGANISATIONAL SECURITY

4.3.1 Security requirements in outsourcing contracts

- **Legal requirements**
- **Awareness**
- **Integrity and logical controls – restrict and limit access**
- **Availability of services in the event of a disaster**
- **The right to audit**

5) Asset Classification and Control

5.1 ACCOUNTABILITY FOR ASSETS

- **Inventory of assets (5.1.1)**

5) Asset classification and control

5.2 INFORMATION CLASSIFICATION

- **Classification guidelines (5.2.1)**
- **Information labeling and handling (5.2.2)**

- **Copying**
- **Storage**
- **Transmission by post, fax, E-mail**
- **Transmission by spoken word , Mobile phone ,voicemail , answering machines**
- **destruction**

6) Personnel security

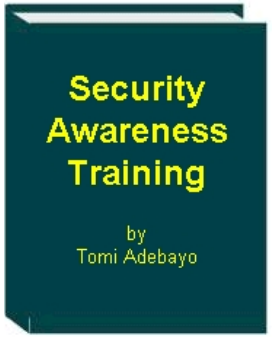
6.1 Security in Job definition and Resourcing

- **Including security in job responsibilities (6.1.1)**
- **Personnel screening and policy (6.1.2)**
- **Confidentiality agreements (6.1.3)**
- **Terms and conditions of employment (6.1.4)**

6) Personnel security

6.2 USER TRANNING

- **Information security education and training (6.2.1)**



6) Personnel security

6.3 RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS

- **Reporting security incidents (6.3.1)**
- **Reporting security weaknesses (6.3.2)**
- **Reporting software malfunctions (6.3.3)**
- **Learning from incidents (6.3.4)**
- **Disciplinary process (6.3.5)**

7) Physical and Environmental Security

7.1 SECURE AREAS

- **Physical security perimeter (7.1.1)**
- **Physical entry controls (7.1.2)**
- **Securing offices , rooms and facilities (7.1.3)**
- **Working in secure areas (7.1.4)**
- **Isolated delivery and loading areas (7.1.5)**
  - from the risk assessment

Access Control Terminal

7) Physical and Environmental Security

7.2 EQUIPMENT SECURITY

- **Equipment siting and protection (7.2.1)**
- **Power supplies (7.2.2)**
- **Cabling security (7.2.3)**
- **Equipment maintenance (7.2.4)**
- **Security of equipment off-premises(7.2.5)**
- **Secure disposal or re-use of equipment (7.2.6)**

7) Physical and environmental security

7.3 GENERAL CONTROLS

- **Clear disk and clear screen policy (7.3.1)**
- **Removal of property (7.3.2)**

8) Communications and Operations Management

8.1 OPERATIONAL PROCUDURES AND RESPONSIBILITIES

- **Documented operating procedures (8.1.3)**
- **Segregation of duties (8.1.4)**
- **Separation of development and operational facilities (8.1.5)**
- **External facilities management (8.1.6)**

8) Communications and Operations Management

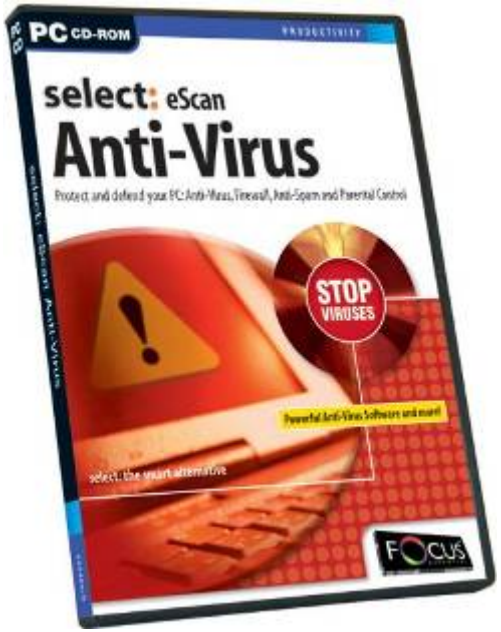
8.2 SYSTEM PLANNING AND ACCEPTANCE

- **Capacity planning (8.2.1)**
- **System acceptance (8.2.2)**

8.3 PROTECTION AGAINTS

MALICIOUS SOFTWARE

- **controls against malicious software (8.3.1)**



8.4 HOUSEKEEPING

- **Information back-up (8.4.1)**
- **Operator logs (8.4.2)**
- **Fault logging (8.4.3)**

8.5 NETWORK MANAGEMENT

- **Network controls (8.5.1)**

8.6 MEDIA HANDLING AND SECURITY

- **Management of removable computer media (8.6.1)**
- **Disposal of media (8.6.2)**
- **Information handling procedures (8.6.3)**
- **Security of system Documentation (8.6.4)**

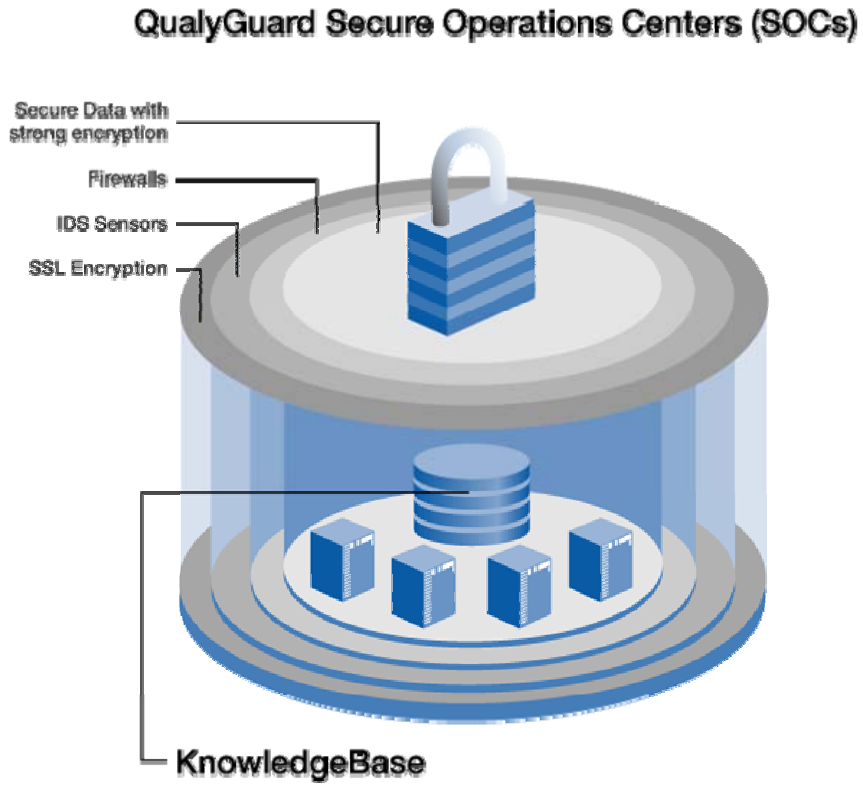
8.7 EXCHANGES OF INFORMATION AND SOFTWARE

- **Information and software exchange agreements (8.7.1)**
- **Security of media in transit (8.7.2)**
- **Electronic commerce security (8.7.3)**
- **Security of electronic mail (8.7.4)**
- **Security of electronic offices systems (8.7.5)**
- **Publicly available system (8.7.6)**
- **Other forms of Information exchange (8.7.7)**

9) Access Control

9.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL

- **Access control policy (9.1.1)**
  - **Policy and business requirements (9.1.1)**
  - **Access control rules (9.1.1.2)**



9) Access Control

9.2 USER ACCESS MANAGEMENT

- **User registration (9.2.1)**
- **Privilege management (9.2.3)**
- **User password management (9.2.3)**
- **Review of user access rights (9.2.4)**

9) Access Control

9.3 USER RESPONSIBILITIES

- **Password use (9.3.1)**
- **Unattended user equipment (9.3.2)**

9) Access Control

9.4 NETWORK ACCESS CONTROL

- **Policy on use of network services (9.4.1)**
- **Enforced path (9.4.2)**
- **User authentication for external connections (9.4.3)**
- **Node authentication (9.4.4)**
- **Remote diagnostic port protection**
- **Segregation in networks (9.4.6)**
- **Network Connection Control (9.4.7)**
- **Network Routing Control (9.4.8)**
- **Security of Network Services (9.4.9)**

9) Access Control

9.5 Operating System Access Control

- **Automatic terminal identification (9.5.1)**
- **Terminal Log-on procedures (9.5.2)**
- **User identification and authentication (9.5.3)**
- **Password management system (9.5.4)**
- **Use of system utilities (9.5.5)**
- **Duress alarm to safeguard users (9.5.6)**
- **Terminal time-out (9.5.7)**
- **Limitation of connection time (9.5.8)**

9) Access Control

9.6 Application access control

- **Information access restriction (9.6.1)**
- **Sensitive system isolation (9.6.2)**

9) Access Control

9.7 MONITORING SYSTEM ACCESS AND USE

- **Event logging (9.7.1)**
- **Monitoring system use (9.7.2)**
  - **Procedures and areas of risk (9.7.2.1)**
  - **Risk factors (9.7.2.2)**
  - **Logging and reviewing events (9.7.2.3)**
- **Clock synchronization (9.7.3)**

10) Systems Development and Maintenance

10.1 SECURITY REQUIREMENTS OF SYSTEMS

- Security requirement analysis and specification

10.2 SECURITY IN APPLICATION SYSTEMS

- Input data validation (10.2.1)
- Control of internal processing (10.2.2)
  - Areas of risk (10.2.2.1)
  - Checks and controls (10.2.2.2)
- Message authentication (10.2.3)
- Output data validation (10.2.4)

10) Systems Development and Maintenance

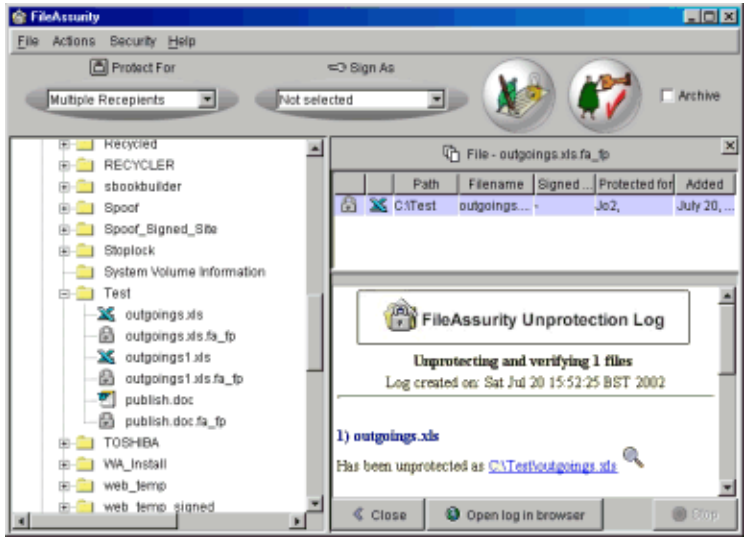
10.3 CRYPTOGRAFIC CONTROLS

- **Policy on the use of cryptographic controls (10.3.1)**
- **Encryption (10.3.2)**
- **Digital signatures (10.3.3)**
- **Non-repudiation services (10.3.4)**
- **Key management (10.3.5)**
    - **Protection of cryptographic keys (10.3.5.1)**
    - **Standards, procedures and methods (10.3.5.2)**

10) Systems Development and Maintenance

10.4 SECURITY SYSTEM FILES

- **Control of operation of software (10.4.1)**
- **Protection of system test data (10.4.2)**
- **Access control to program source library (10.4.3)**



10) Systems Development and Maintenance

10.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

- **Change control procedures (10.5.1)**
- **Technical review of operating system changes (10.5.2)**
- **Restrictions on changes to software packages (10.5.3)**
- **Covet channels and Trojan Code (10.5.4)**
- **Outsourced software development (10.5.5)**

11) Business Continuity Management

11.1 ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

- **Business Continuity management process (11.1.1)**
- **Business Continuity and impact analysis (11.1.2)**
- **Writing and implementing continuity plans (11.1.3)**
- **Business Continuity planning framework (11.1.4)**
- **Testing, maintaining and re-assessing business continuity plans (11.1.5)**
  - **Testing and plans (11.1.5.1)**
  - **Maintaining and re-assessing the plans (11.1.5.2)**

Based on the Risk Analysis and everything else!

12) Compliance

12.1 COMPLIANCE WITH LEGAL REQUIREMENTS

- **Identification of applicable legislation (12.1.1)**
- **Intellectual property rights, IPR (12.1.2)**
  - **Copyright (12.1.2.1), Software Copyright (12.1.2.2)**
- **Safeguarding of organizational records (12.1.3)**
- **Data protection and privacy of personal information (12.1.4)**
- **Prevention of misuse of information processing facilities (12.1.5)**
- **Regulation of cryptographic controls (12.1.6)**
- **Collection of evidence (12.1.7) – not valid in all countries**

12) Compliance

12.2 REVIEWS OF SECURITY POLICY AND TECHNICAL COMPLIANCE

- **Compliance with security policy (12.2.1)**
- **Technical compliance checking (12.2.2)**

12.3 SYSTEM AUDIT CONSIDERATIONS

- **System audits controls (12.3.1)**
- **Protection of system audit tools (12.3.2)**