Management of Information Security, 4th Edition

Chapter 6

Security Management Models

Objectives

- Describe the dominant InfoSec blueprints, frameworks, and InfoSec management models.
- Explain why access control is an essential element of InfoSec management
- Recommend an InfoSec management model and explain how it can be customized to meet the needs of a particular organization
- Describe the fundamental elements of key InfoSec management practices

Blueprints, Frameworks, and Security Models

- Blueprint - describes existing controls and identifies other necessary security controls
- Framework - the outline of the more thorough blueprint
- Security model - a generic blueprint offered by a service organization

Blueprints, Frameworks, and Security Models (continued)

- Another way to create a blueprint:
  - To look at the paths taken by other organizations
- Benchmarking: the comparison of two related measurements

Access Control Models Part 1

- Access controls - regulate the admission of users into trusted areas of the organization
- Access control is maintained by means of:
  - A collection of policies
  - Programs to carry out those policies
  - Technologies to enforce policies

Access Control Models Part 2

- General application of access control comprises four processes:
  - Identification - obtaining identity of the entity requesting access to a logical or physical area
  - Authentication - confirming the identity
  - Authorization - determining which actions an authenticated entity can perform in that physical or logical area
  - Accountability - documenting the activities of the authorized individual and systems

Access Control Models Part 3

- Access control is built on several key principles:
  - Least privilege - member of the organization can access the minimum amount of information for the minimum amount of time necessary
  - Need-to-know - limits a user's access to the specific information required to perform the currently assigned task
  - Separation of duties - requires that significant tasks be split up in such a way that more than one individual is responsible for their completion

Categories of Access Control

- A number of approaches are used to categorize access control methodologies

Table 6-1 Categories of access control

	Deterrent	Preventative	Detective	Corrective	Recovery	Compensating
Management	Policies	Registration procedures	Periodic violation report reviews	Employee or account termination	Disaster recovery plan	Separation of duties, job rotation
Operational	Warning signs	Gates, fences, and guards	Sentries. CCTVs	Fire suppression systems	Disaster recovery procedures	Defense in depth
Technical	Warning banners	Login systems. Kerberos	Log monitors and IDPSs	Forensics procedures	Data backups	Key logging and keystroke monitoring

Mandatory Access Controls

- A mandatory access control (MAC) - is required and is structured and coordinated within a data classification scheme that rates each collection of information
- When MACs are implemented:
  - Users and data owners have limited control over access to information resources

Data Classification Model

- The U.S. military uses a five-level classification scheme:
  - *Unclassified data*
  - *Sensitive but unclassified (SBU) data*
  - *Confidential data*
  - *Secret data*
  - *Top secret data*

Data Classification Model (continued)

- An organization can protect its sensitive information with a simple scheme like the following:
  - *Public* - for general public dissemination
  - *For official use only* - not for public release but not sensitive
  - *Sensitive* - important information that , if compromised, could embarrass the organization
  - *Classified* - essential and confidential information
    - Disclosure of which could severely damage the well-being of the organization

Security Clearances

- **Security clearance** structure - each user of an information asset is assigned an authorization level that identifies the level of information classification he or she can access
- Most organizations have developed a set of roles and a corresponding security clearance

Managing Classified Information Assets

- Managing an information asset includes all aspects of its life cycle
  - From specification to design, acquisition, implementation, use, storage, distribution, backup, recovery, retirement, and destruction
- “Clean desk policy” - requires each employee to secure all information in its appropriate storage container at the end of every business day

Nondiscretionary Controls

- Nondiscretionary controls - determined by a central authority in the organization and can be based on:
  - **Role-based controls** - tied to the role that a user performs
  - **Task-based controls** - tied to a particular assignment or responsibility

Other Forms of Access Control

- Other models of access control include:
  - *Content-dependent access controls* - access may be dependent on its content
  - *Constrained user interfaces* - designed specifically to restrict what information an individual user can access
  - *Temporal (time-based) isolation* - access to information is limited by a time-of-day constraint

Security Architecture Models

- Security architecture models - illustrate InfoSec implementations and can help organizations quickly make improvements through adaptation
- Some models are:
  - Implemented into computer hardware and software
  - Implemented as policies and practices
  - Focused on the confidentiality of information
  - Focused on the integrity of the information as it is being processed

Trusted Computing Base Part 1

- **Trusted Computer System Evaluation Criteria (TCSEC)** - an older standard that defines the criteria for assessing the access controls in a computer system
- TCSEC defines a **trusted computing base (TCB)** as the combination of all hardware, firmware, and software responsible for enforcing security policy

Trusted Computing Base Part 2

- **Covert channels** - unauthorized or unintended methods of communications hidden inside a computer system

Trusted Computing Base Part 3

- Products evaluated under TCSEC are assigned one of the following levels of protection
  - *D: Minimal protection*
  - *C: Discretionary protection*
  - *B: Mandatory protection*
  - *A: Verified protection*

Information Technology System Evaluation Criteria

- Information Technology System Evaluation Criteria (ITSEC) - an international set of criteria for evaluating computer system
- ITSEC rates products on a scale of E1 (lowest level) to E6 (highest level)

The Common Criteria

- **Common Criteria for Information Technology Security Evaluation** - an international standard for computer security certification
  - Often called “Common Criteria” or “CC”
  - Considered the successor to TCSEC and ITSEC
- CC terminology includes
  - *Target of Evaluation (ToE)*
  - *Protection Profile (PP)*
  - *Security Target (ST)*
  - *Security Functional Requirements (SFRs)*
  - *Evaluation Assurance Levels (EAL)*

The Common Criteria (continued)

- EAL is typically rated on the following scale:
  - *EAL1: Functionally Tested*
  - *EAL2: Structurally Tested*
  - *EAL3: Methodically Tested and Checked*
  - *EAL4: Methodically Designed, Tested, and Reviewed*
  - *EAL5: Semi-formally Designed and Tested*
  - *EAL6: Semi-formally Verified Design and Tested*
  - *EAL7: Formally Verified Design and Tested*

The ISO 27000 Series

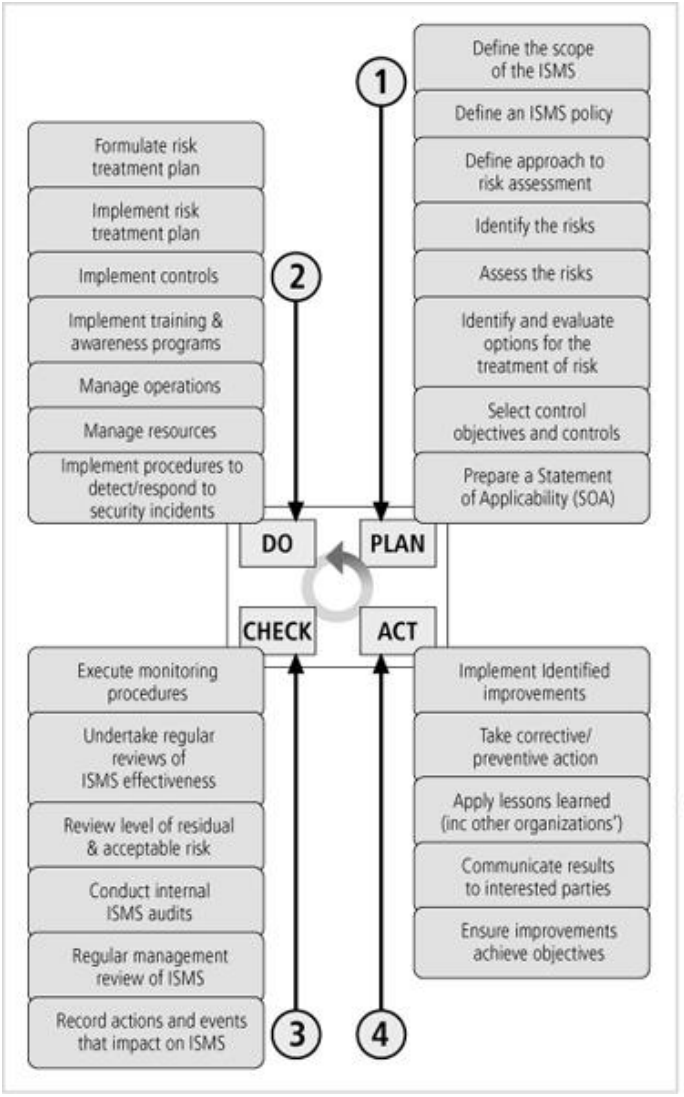
- Information Technology - Code of Practice for Information Security Management - one of the most widely referenced InfoSec management models
  - The Code of Practice was adopted as an international standard framework for InfoSec by the ISO and the IEC as ISO/IEC 17799
  - It was revised in 2005 and in 2007 was renamed ISO 27002
  - Was intended to provide a common basis for developing organizational security standards

Table 6-2 Sections of the ISO/IEC 27002

- Structure
- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resource Security
- Physical and Environmental Security
- Communications and Operations
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Source: 27000.org

Figure 6-2 ISO/IEC 27001 major process steps



NIST Security Models

- Advantages of NIST security models over many other sources of security information:
  - They are publicly available at no charge
  - They have been available for some time and have been broadly reviewed by the government and industry professionals

NIST Special Publication 800-12

- SP 800-12: Computer Security Handbook - an excellent reference and guide for routine management of InfoSec
- SP 800-12 provides for:
  - *Accountability*
  - *Awareness*
  - *Ethics*
  - *Multidisciplinary*
  - *Proportionality*
  - *Integration*

NIST Special Publication 800-12 (continued)

- SP 800-12 provides for (cont'd):
  - *Timeliness*
  - *Reassessment*
  - *Democracy*
- SP 800-12 organizes controls into three categories:
  - Management controls
  - Operational controls
  - Technical controls

NIST Special Publication 800-14 Part 1

- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
  - Can direct the security team in the development of a security blueprint

NIST Special Publication 800-14 Part 2

- Significant points made in NIST SP 800-14:
  - *Security supports the mission of the organization*
  - *Security is an integral element of sound management*
  - *Security should be cost-effective*
  - *Systems owners have security responsibilities outside their own organizations*
  - *Security responsibilities and accountability should be made explicit*
  - *Security requires a comprehensive and integrated approach*

NIST Special Publication 800-14 Part 3

- Significant points made in NIST SP 800-14 (cont'd):
  - *Security should be periodically reassessed*
  - *Security is constrained by societal factors*

Control Objectives for Information and Related Technology

- "Control Objectives for Information and Related Technology" (COBIT)
  - Provides advice about the implementation of sound controls and control objectives for InfoSec

Control Objectives for Information and Related Technology (continued)

- COBIT 5 provides five principles focused on the governance and management of IT:
  - *Meeting Stakeholder Needs*
  - *Covering the Enterprise End-to-End*
  - *Applying a Single, Integrated Framework*
  - *Enabling a Holistic Approach*
  - *Separating Governance from Management*

Committee of Sponsoring Organizations

- Committee of Sponsoring Organizations (COSO) of the Treadway Commission
  - Another control-based model

Committee of Sponsoring Organizations (continued)

- The COSO framework is built on five interrelated components:
  - *Control environment*
  - *Risk assessment*
  - *Control activities*
  - *Information and communication*
  - *Monitoring*

Information Technology Infrastructure Library

- Information Technology Infrastructure Library (ITIL)
  - A collection of methods and practices for managing the development and operation of IT infrastructures
- ITIL has produced a series of books
  - Each of which covers an IT management topic

Information Security Governance Framework

- The Information Security Governance Framework is a managerial model provided by an industry working group
- The framework provides guidance in the development and implementations of an organizational InfoSec governance structure
- The framework also specifies that each independent organizational unit should develop, document, and implement in InfoSec program consistent with accepted security practices

Summary Part 1

- A framework is the outline of a more thorough blueprint, used in the creation of the InfoSec environment
- Access controls regulate the admission of users into trusted areas of the organization
- Access control is built on the principles of least privilege, need-to-know, and separation of duties
- Approaches to access control include preventative, deterrent, detective, corrective, recovery, and compensating
- Mandatory access controls (MACs) are required by the system that operate within a data classification and personnel clearance scheme

Summary Part 2

- Nondiscretionary controls are determined by a central authority in the organization and can be based on roles or on a specified set of tasks
- Security architecture models illustrate InfoSec implementations and can help organizations make quick improvements through adaptation
- One of the most widely referenced security models is “ISO/IEC 27001: 2005 Information Technology - Code of Practice for InfoSec Management”
  - Designed to give recommendations for InfoSec management

Summary Part 3

- “Control Objectives for Information and Related Technology” (COBIT) provides advice about the implementation of sound controls and control objectives for InfoSec
- The Information Security Governance Framework is a managerial model provided by an industry working group that provides guidance in the development and implementation of an organizational InfoSec governance structure