Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts.

– William O. Douglas, U.S. Supreme Court Justice
Objectives Chapter 6

- Describe the dominant information security blueprints, frameworks and information security management models, including U.S. government-sanctioned models.

- Explain why access control is an essential element of information security management.

- Select an information security management model, and customize it to meet the needs of a particular organization.

- Implement the fundamental elements of key information security management practices.

- Discuss emerging trends in the certification and accreditation of U.S. federal IT systems.
Blueprints, Frameworks, and Security Models

• To create or maintain a secure environment
  – Design a working security plan
  – Implement a management model to execute and maintain the plan

• Begin by creating or validating a security framework
  – Create an information security blueprint to describe existing controls and identify other necessary security controls
Blueprints, Frameworks, and Security Models (cont’d.)

• Framework
  – The outline of the more thorough blueprint
  • Which is the basis for the design, selection, and implementation of all subsequent security controls

• Most organizations draw from established security models and practices to develop a blueprint or methodology
  – A security model is a generic blueprint offered by a service organization
Access Control Models

• **Access controls**
  – Regulate the admission of users into trusted areas of the organization
  • Both the logical access to the information systems and the physical access to the organization’s facilities
  – Maintained by means of a collection of policies, programs to carry out those policies, and technologies that enforce policies
Access Control Models (cont’d.)

• Key principles of access control

1) Least privilege
   • The principle by which members of the organization can access the minimum amount of information for the minimum amount of time necessary to perform their required duties

2) Need to Know
   • Limits a user’s access to the specific information required to perform the currently assigned task, and not merely to the category of data required for a general work function

3) Separation of Duties
   • A control requiring that significant tasks be split up in such a way that more than one individual is responsible for their completion
Categories of Access Control

1) Preventative – avoid an incident
2) Deterrent – prevent an initial incident
3) Detective – detect and identify incident
4) Corrective – mitigate damage done
5) Recovery – restore operation
6) Compensating – resolve shortcomings
Categories of Access Control

- NIST* Access Control categories are based on operational impact to the organization
  - A. Management
  - B. Operational (or administrative)
  - C. Technical

Table 6-1 Examples of controls by operational level and inherent characteristics
Categories of Access Control

• **Mandatory Access Controls (MACs)**
  
  – Structured and coordinated within a data classification scheme that **rates each collection of information as well as each user**
  
  – These ratings are often referred to as sensitivity levels
  
  – When MACs are implemented, users and data owners have **limited control** over access to information resources
Categories of Access Control

• Data classification model
  – Data owners must classify the information assets for which they are responsible and review the classifications periodically
  – Example of classification types:
    • Public
    • For official use only
    • Sensitive
    • Classified
Categories of Access Control

• Data classification model (cont’d.)
  – The U.S. military classification scheme relies on a more complex five-level classification scheme as defined in Executive Order 12958:
    • Unclassified data
    • Sensitive but unclassified (SBU) data
    • Confidential data
    • Secret data
    • Top secret data
Categories of Access Control

• **Security clearance structure**
  
  – Each user of an information asset is assigned an authorization level
    
    • Indicates the level of information classification they may access
  
  – Most organizations have developed roles and corresponding security clearances
    
    • Individuals are assigned into groups that correlate with the classifications of the information assets they need for their work
Categories of Access Control

• Security clearance structure (cont’d.)
  – In the need-to-know principle, regardless of one’s security clearance, an individual is not allowed to view data simply because it falls within that individual’s level of clearance
  • Must need to know the information
Categories of Access Control

• Managing an information asset
  – Considering its storage, distribution, portability, and destruction
  – An information asset that has a classification designation other than unclassified or public must be clearly marked as such
    • Must be available only to authorized individuals
  – To maintain the confidentiality of classified documents, managers can implement a clean desk policy
Categories of Access Control

• Managing an information asset (cont’d.)
  – When copies of classified information are no longer valuable or too many copies exist, care should be taken to destroy them properly to discourage dumpster diving
Categories of Access Control

Figure 6-1 Military data classification cover sheets
Categories of Access Control

• Lattice-Based Access Controls
  – A variation on the MAC form of access control
  – Assigns users a matrix of authorizations for particular areas of access
  – The level of authorization can vary
    • Depending on individual’s classification authorization for each group of information assets
  – Lattice structure contains subjects and objects
    • Boundaries associated with each subject/object pair are clearly demarcated
Categories of Access Control

• **Nondiscretionary controls**
  – Determined by a central authority in the organization
  – Can be role-based or task-based

• **Role-based controls** are tied to a particular user’s role in an organization

• **Task-based controls** are tied to a particular assignment or responsibility
Categories of Access Control

- **Discretionary Access Controls (DACs)**
  - Implemented at the option of the data user
  - Users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access the resources
  - Most *personal computer operating systems* are designed based on the DAC model
  - One discretionary model is rule-based access controls where access is granted based on a set of rules specified by the central authority
Categories of Access Control

• Other forms of access control
  ▪ Content-dependent access controls
  ▪ Constrained user interfaces
  ▪ Temporal (time-based) isolation
Security Architecture Models

• Illustrate InfoSec implementations
• Can help organizations quickly make improvements through adaptation
  – Some models are implemented into computer hardware and software
  – Some are policies and practices
  – Some are implemented in both
  – Some models focus on the confidentiality of information, while others focus on the integrity of the information as it is being processed
SECURITY ARCHITECTURE MODEL

1) Trusted Computing Base Model (Authorization)
2) Bell-LaPadula Confidentiality Model (confidentiality)
3) Biba Integrity Model (integrity)
4) Clark-Wilson Integrity Model (Access Control (AC))
5) Graham-Denning Access Control Model (AC)
6) Harrison-Ruzzo-Ullman (AC)
7) Brewer-Nash (Chinese Wall) (AC – prevent conflict)
8) The Common Criteria
1) Trusted Computing Base

• Trusted Computer System Evaluation Criteria (TCSEC)
  – U.S. Government Department of Defense standard that defines *criteria for assessing access controls in a computer system*
  – Part of a larger series of standards collectively referred to as the Rainbow Series, due to the color-coding used to uniquely identify each document
    • Also known as the “Orange Book” and is considered the cornerstone of the series
Trusted Computing Base (cont’d.)

- Trusted computing base (TCB)
  - The combination of all hardware, firmware, and software responsible for enforcing the security policy
    - In this context, security policy refers to the rules of configuration for a system, rather than a managerial guidance document
  - Made up of the hardware and software that has been implemented to provide security for a particular information system
Trusted Computing Base (cont’d.)

• Reference monitor
  – A conceptual object
  – The piece of the system that manages access controls
    • It mediates all access to objects by subjects
  – Systems administrators must be able to audit or periodically review the reference monitor to ensure it is functioning effectively, without unauthorized modification
Trusted Computing Base (cont’d.)

• Covert channels
  – Unauthorized or unintended methods of communications hidden inside a computer system

• Types of covert channels
  – Storage channels, which communicate by modifying a stored object
  – Timing channels, which transmit information by managing the relative timing of events
2) Bell-LaPadula Confidentiality Model

• A state machine model that helps ensure the confidentiality of an information system
  – Using mandatory access controls (MACs), data classification, and security clearances

• A state machine model follows a conceptual approach in which the state of the content of the system being modeled is always in a known secure condition
  – This kind of model is provably secure
Bell-LaPadula Confidentiality Model (cont’d.)

• A system that serves as a reference monitor compares the level of classification of the data with the clearance of the entity requesting access
  – It allows access only if the clearance is equal to or higher than the classification

• BLP security rules prevent information from being moved from a level of higher security level to a level of lower security
Bell-LaPadula Confidentiality Model (cont’d.)

• Access modes can be one of two types
  – Simple security
    • Prohibits a subject of lower clearance from reading an object of higher classification, but allows a subject with a higher clearance level to read an object at a lower level (read down)
  – The * (star) property
    • The * property (the write property) prohibits a high-level subject from sending messages to a lower-level object
  – Subjects can read down and objects can write or append up
3) Biba Integrity Model

• Similar to Bell-LaPadula
• Provides access controls to ensure that objects or subjects cannot have less integrity as a result of read/write operations
• Ensures no information from a subject can be passed on to an object in a higher security level
  – This prevents contaminating data of higher integrity with data of lower integrity
Biba Integrity Model (cont’d.)

• Assigns integrity levels to subjects and objects using two properties
  – The simple integrity (read) property
    • Permits a subject to have read access to an object only if the security level of the subject is equal to or lower than the level of the object
  – The integrity * (write) property
    • Permits a subject to have write access to an object only if the security level of the subject is equal to or higher than that of the object
4) Clark-Wilson Integrity Model

- Built upon principles of change control rather than integrity levels
- Designed for the commercial environment
- Its change control principles
  - No changes by unauthorized subjects
  - No unauthorized changes by authorized subjects
  - The maintenance of internal and external consistency
Clark-Wilson Integrity Model (cont’d.)

• Establishes a system of subject-program-object relationships
  – Such that the subject has no direct access to the object
  – The subject is required to access the object using a well-formed transaction using a validated program

• Provides an environment where security can be proven through separated activities, each of which is provably secure
Clark-Wilson Integrity Model (cont’d.)

• CWI model controls
  – Subject authentication and identification
  – Access to objects by means of well-formed transactions
  – Execution by subjects on a restricted set of programs

• Elements of the CWI model
  – Constrained data item (CDI)
    • The integrity of this data item is protected
Clark-Wilson Integrity Model (cont’d.)

• Elements of the CWI model (cont’d.)
  – Unconstrained data item
    • Data not controlled by Clark-Wilson
    • Non-validated input or any output
  – Integrity verification procedure (IVP)
    • Procedure that scans data and confirms its integrity
  – Transformation procedures (TPs)
    • Procedures that only allow changes to a constrained data item
5) Graham-Denning Access Control Model

• Composed of three parts
  – A set of objects
  – A set of subjects (a process and a domain)
    • The domain is the set of constraints controlling how subjects may access objects
  – A set of rights

• **Primitive protection rights**
  – Create or delete object, create or delete subject
  – Read, grant, transfer and delete access rights
6) Harrison-Ruzzo-Ullman Model

• Defines a method to allow changes to access rights and the addition and removal of subjects and objects
  – A process that the Bell-LaPadula model does not have
  – Since systems change over time, their protective states need to change

• Built on an access control matrix

• Includes a set of generic rights and a specific set of commands
7) Brewer-Nash Model (Chinese Wall)

- Also known as a Chinese Wall
- Designed to prevent a conflict of interest between two parties
- Requires users to select one of two conflicting sets of data, after which they cannot access the conflicting data
SECURITY MANAGEMENT MODEL

1) ISO 27000 Series
2) NIST Security Model
3) COBIT (Control Objectives for Information and Related Technology)
4) COSO (Committee Of Sponsoring Organisations of the Treadway Commission)
5) ITIL (Information Technology Infrastructure Library)
6) ISGF (Information Security Governance Framework)
The ISO 27000 Series

• Information Technology – **Code of Practice for Information Security Management**
  – One of the most widely referenced and discussed security models
  – Originally published as British Standard 7799 and then later as ISO/IEC 17799
  – Since been renamed ISO/IEC 27002

• Establishes guidelines for initiating, implementing, maintaining, and improving information security management
The ISO 270000 Series (cont’d.)

• ISO/IEC 27002 has 133 possible controls
  – Not all of which must be used
  – Need to identify which are relevant

• Each section includes four categories of information:
  – One or more objectives
  – Controls relevant to the achievement of the objectives
  – Implementation guidance
  – Other information
• Many countries did not originally adopted the model
  – Including the US, Germany, and Japan

• Claims of fundamental flaws
  – Global InfoSec community has not defined any justification for the code of practice identified
  – Model lacks the necessary measurement precision of a technical standard
  – No reason to believe the model is more useful than any other approach
  – Not as complete as other frameworks
  – Perceived as being hurriedly prepared, given the tremendous impact that its adoption could have on industry information security controls
The ISO 27000 Series (cont’d.)

• ISO/IEC 27002 Sections
  – Security policy
  – Organization of information security
  – Asset management
  – Human resources security
  – Physical and environmental security
  – Communications and operations management
  – Access control
  – Information systems acquisition, development and maintenance
The ISO 27000 Series (cont’d.)

• ISO/IEC 27002 Sections (cont’d.)
  – Information security incident management
  – Business continuity management
  – Compliance
The ISO 27000 Series (cont’d.)

Figure 6-3 ISO/IEC 27001 Plan-Do-Check-Act
The ISO 27000 Series (cont’d.)

• ISO/IEC 27001:2005
  -The InfoSec Management System - Plan
    1. Define the scope of the ISMS
    2. Define an ISMS policy
    3. Define the approach to risk assessment
    4. Identify the risks
    5. Assess the risks
    6. Identify and evaluate options for the treatment of risk
    7. Select control objectives and controls
    8. Prepare a statement of applicability (SOA)
The ISO 27000 Series (cont’d.)


  9. Formulate a risk treatment plan
  10. Implement the risk treatment plan
  11. Implement controls
  12. Implement training and awareness programs
  13. Manage operations
  14. Manage resources
  15. Implement procedures to detect and respond to security incidents
The ISO 27000 Series (cont’d.)

  16. Execute monitoring procedures
  17. Undertake regular reviews of ISMS effectiveness
  18. Review the level of residual and acceptable risk
  19. Conduct internal ISMS audits
  20. Undertake regular management review of the ISMS
  21. Record actions and events that impact an ISMS
The ISO 27000 Series (cont’d.)

  22. Implement identified improvements
  23. Take corrective or preventive action
  24. Apply lessons learned
  25. Communicate results to interested parties
  26. Ensure improvements achieve objectives
The ISO 27000 Series (cont’d.)

<table>
<thead>
<tr>
<th>ISO 27000 Series Standard</th>
<th>Status</th>
<th>Title or Topic</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>27000</td>
<td>May 2009</td>
<td>Series Overview and Terminology</td>
<td>Defines terminology and vocabulary for the standard series</td>
</tr>
<tr>
<td>27001</td>
<td>2005</td>
<td>Information Security Management System Specification</td>
<td>Drawn from BS 7799:2</td>
</tr>
<tr>
<td>27002</td>
<td>July 2007</td>
<td>Code of Practice for Information Security Management</td>
<td>Renamed from ISO/IEC 17799, drawn from BS 7799:1</td>
</tr>
<tr>
<td>27003</td>
<td>Planned</td>
<td>Information Security Management Systems Implementation Guidelines</td>
<td>Expected late 2009 or 2010</td>
</tr>
<tr>
<td>27004</td>
<td>Planned</td>
<td>Information Security Measurements and Metrics</td>
<td>Expected in late 2009 or 2010</td>
</tr>
<tr>
<td>27005</td>
<td>2008</td>
<td>ISMS Risk Management</td>
<td></td>
</tr>
<tr>
<td>27006</td>
<td>2007</td>
<td>Requirements for Bodies Providing Audit and Certification of an ISMS</td>
<td>Is largely intended to support the accreditation of certification bodies providing ISMS certification</td>
</tr>
<tr>
<td>27007</td>
<td>Planned</td>
<td>Guidelines for ISMS Auditing</td>
<td>Focuses on management systems</td>
</tr>
<tr>
<td>27008</td>
<td>Planned</td>
<td>Guidelines for ISMS Auditing</td>
<td>Focuses on management controls</td>
</tr>
<tr>
<td>27011</td>
<td>2008</td>
<td>Information Security Guidelines for the Telecommunications Industry</td>
<td></td>
</tr>
<tr>
<td>27014</td>
<td>Planned</td>
<td>Information Security Governance Framework</td>
<td></td>
</tr>
<tr>
<td>27015</td>
<td>Planned</td>
<td>Information Security Management Guidelines for the Finance and Insurance Sectors</td>
<td></td>
</tr>
<tr>
<td>27032</td>
<td>Planned</td>
<td>Guideline for Cybersecurity</td>
<td></td>
</tr>
<tr>
<td>27034</td>
<td>Planned</td>
<td>Guideline for Application Security</td>
<td></td>
</tr>
</tbody>
</table>

Table 6-4 ISO 27000 Series current and planned standards
NIST Security Models

• Notable advantages of NIST documents
  – Publicly available at no charge
  – Have been available for some time
  – Have been broadly reviewed by government and industry professionals
NIST Security Models (cont’d.)

• Examples
  – SP 800-12, *Computer Security Handbook*
  – SP 800-14, *Generally Accepted Security Principles & Practices*
  – SP 800-30, *Risk Management for Information Technology Systems*
NIST Security Models (cont’d.)

• NIST SP 800-12: *Computer Security Handbook*
  – Excellent reference and guide for the routine management of information security
  – Little guidance provided on design and implementation of new security systems
  – Use as supplement to gain a deeper understanding of background and terminology
NIST Security Models (cont’d.)

• NIST SP 800-12: *Computer Security Handbook* (cont’d.)
  – Lays out the NIST philosophy on security management by identifying 17 controls organized into three categories
    • Management controls: addresses security topics that can be characterized as managerial
    • Operational controls: addresses security controls that focus on controls implemented and executed by people (as opposed to systems)
    • Technical controls: focuses on security controls that the computer system executes
NIST Security Models (cont’d.)

• NIST Special Publication 800-14: *Generally Accepted Principles and Practices for Securing Information Technology Systems*
  – Describes best practices useful in the development of a security blueprint
  – Describes principles that should be integrated into information security processes
  – Documents 8 points and 33 principles
NIST Security Models (cont’d.)

• Key points
  – Security supports organization’s mission
  – Security is integral to sound management
  – Security should be cost-effective
  – Systems owners have security responsibilities outside their own organizations
  – Security responsibilities and accountability should be explicit
  – Security requires a comprehensive and integrated approach
  – Security should be periodically reassessed
  – Security is constrained by societal factors
NIST Security Models (cont’d.)

• Principles of NIST SP 800-14
  1. Establish a sound security policy as the foundation for design
  2. Treat security as an integral part of the overall system design
  3. Clearly delineate the physical and logical security boundaries governed by associated security policies
  4. Reduce risk to an acceptable level
  5. Assume that external systems are insecure
NIST Security Models (cont’d.)

• Principles of NIST SP 800-14 (cont’d.)
  6. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness
  7. Implement layered security (ensure no single point of vulnerability)
  8. Implement tailored system security measures to meet organizational security goals
  9. Strive for simplicity
NIST Security Models (cont’d.)

- Principles of NIST SP 800-14 (cont’d.)
  - 10. Design and operate an IT system to limit vulnerability and to be resilient in response
  - 11. Minimize the system elements to be trusted
  - 12. Implement security through a combination of measures distributed physically and logically
  - 13. Provide assurance that the system is, and continues to be, resilient in the face of expected threats
  - 14. Limit or contain vulnerabilities
NIST Security Models (cont’d.)

• Principles of NIST SP 800-14 (cont’d.)
  – 15. Formulate security measures to address multiple overlapping information domains
  – 16. Isolate public access systems from mission critical resources
  – 17. Use boundary mechanisms to separate computing systems and network infrastructures
  – 18. Where possible, base security on open standards for portability and interoperability
NIST Security Models (cont’d.)

• Principles of NIST SP 800-14 (cont’d.)
  – 19. Use common language in developing security requirements
  – 20. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations
  – 21. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process
NIST Security Models (cont’d.)

• Principles of NIST SP 800-14 (cont’d.)
  – 22. Authenticate users and processes to ensure appropriate access control decisions both within and across domains
  – 23. Use unique identities to ensure accountability
  – 24. Implement least privilege
  – 25. Do not implement unnecessary security mechanisms
NIST Security Models (cont’d.)

- Principles of NIST SP 800-14 (cont’d.)
  - 26. Protect information while being processed, in transit, and in storage
  - 27. Strive for operational ease of use
  - 28. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability
  - 29. Consider custom products to achieve adequate security
NIST Security Models (cont’d.)

• Principles of NIST SP 800-14 (cont’d.)
  – 30. Ensure proper security in the shutdown or disposal of a system
  – 31. Protect against all likely classes of attacks
  – 32. Identify and prevent common errors and vulnerabilities
  – 33. Ensure that developers are trained in how to develop secure software
NIST Security Models (cont’d.)

• NIST Special Publication 800-18, Rev. 1: *A Guide for Developing Security Plans for Federal Information Systems*
  – Provides detailed methods for assessing, designing, and implementing controls and plans for various sized applications
  – Serves as a guide for the activities described in this chapter, and for the overall information security planning process
  – Includes templates for major application security plans
NIST Security Models (cont’d.)

• Management controls
  – Risk management
  – Review of security controls
  – Life cycle maintenance
  – Authorization of processing (certification and accreditation)
  – System security plan
NIST Security Models (cont’d.)

• Operational controls
  – Personnel security
  – Physical security
  – Production, input/output controls
  – Contingency planning
  – Hardware and systems software
  – Data integrity
  – Documentation
  – Security awareness, training, and education
  – Incident response capability
NIST Security Models (cont’d.)

• Technical controls
  – Identification and authentication
  – Logical access controls
  – Audit trails
NIST Security Models (cont’d.)

• NIST Special Publication 800-30: *Risk Management Guide for Information Technology Systems*
  – Provides a foundation for the development of an effective risk management program
  – Contains the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems
  – Strives to enable organizations to better manage IT-related risks
NIST Security Models (cont’d.)

• RFC 2196 Site Security Handbook
  – Provides a functional discussion of important security issues along with development and implementation details
  – Covers security policies, security technical architecture, security services, and security incident handling
  – Includes discussion of the importance of security policies, and an examination of services, access controls, and other relevant areas
NIST Security Models (cont’d.)

• Control Objectives for Information and Related Technology (COBIT)
  – Provides advice about the implementation of sound controls and control objectives for InfoSec
  – Created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992
NIST Security Models (cont’d.)

• COBIT presents 34 high-level objectives that cover 215 control objectives

• Objectives categorized into four domains:
  – Plan and organize
  – Acquire and implement
  – Deliver and support
  – Monitor and evaluate
NIST Security Models (cont’d.)

• Plan and organize
  – Makes recommendations for achieving organizational goals and objectives through the use of IT
  – 10 controlling objectives (PO1 – PO10)

• Acquire and implement
  – Focuses on specification of requirements
  – Acquisition of needed components
  – Component integration
NIST Security Models (cont’d.)

• Acquire and implement (cont’d.)
  – Examines ongoing maintenance and change requirements
  – 7 controlling objectives (AI1 – AI7)

• Delivery and support
  – Focuses on the functionality of the system and its use to the end user
  – Examines systems applications: including input, processing, and output components
NIST Security Models (cont’d.)

• Delivery and support (cont’d.)
  – Examines processes for efficiency and effective of operations
  – 13 high-level controlling objectives (DS1 – DS13)

• Monitor and evaluate
  – Seeks to examine the alignment between IT systems usage and organizational strategy
NIST Security Models (cont’d.)

• Monitor and evaluate (cont’d.)
  – Identifies the regulatory requirements for which controls are needed
  – Monitors the effectiveness and efficiency of IT systems against the organizational control processes in the delivery and support domain
  – 4 high-level controlling objectives (ME1 – ME4)
10) COSO

• A U.S. private-sector initiative
  – Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence
  – Has established a common definition of internal controls, standards and criteria
  – Helps organizations comply with critical regulations like Sarbanes-Oxley
COSO (cont’d.)

• Built on five interrelated components:
  – Control environment
  – Risk assessment
  – Control activities
  – Information and communication
  – Monitoring
Information Technology Infrastructure Library (ITIL)

• A collection of methods and practices useful for managing the development and operation of information technology infrastructures

• Has been produced as a series of books
  – Each of which covers an IT management topic

• Includes a detailed description of many significant IT-related practices
  – Can be tailored to many IT organizations
Information Security Governance Framework

• A managerial model
  – Provides guidance in the development and implementation of an organizational information security governance structure

• Includes recommendations for the responsibilities of members of an organization
Information Security Governance Framework (cont’d.)

• Recommendations for responsibilities of members of an organization
  – Board of directors/trustees
    • Provide strategic oversight for information security
  – Senior executives
    • Provide oversight of a comprehensive information security program for the entire organization
  – Executive team members
    • Oversee the organization’s security policies and practices
Information Security Governance Framework (cont’d.)

• Recommendations for responsibilities of members of an organization (cont’d.)
  – Senior managers
    • Provide information security for the information and information systems that support the operations and assets under their control
  – All employees and users
    • Maintain security of information and information systems accessible to them
Summary

• Introduction

• Security Management Models
  – System Models (BLP, Biba, CWI, HRU, BN, etc).
  – ISO 27000 Series
  – NIST Models
  – Others (COBIT, COSO, ITIL, Corporate Governance)