Security Management

SCSR4473

Session 1516-2

by

Dr. Siti Hajar Othman

Department of Computer Science, Faculty of Computing, UTM

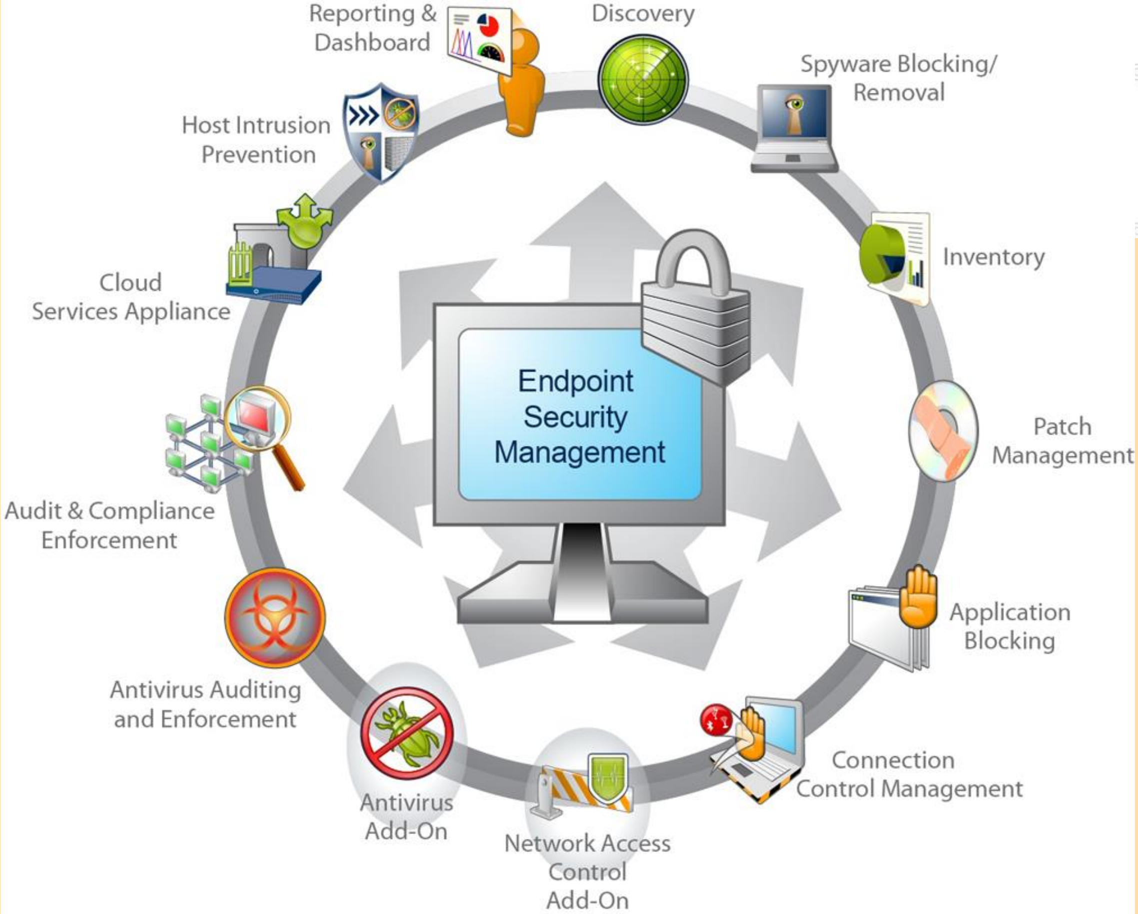
Contact: 🖃 hajar@fc.utm.my/ ☎ 07-553 32372 / Office: N28 347-04

Class Grading

- **Class Marks (45%)**
  - –Quizzes – 2 (5% each) = (10%)
  - –Assignments – 2 (5% each) = (10%)
  - –Presentation – 2 (5% each) = (10%)
  - –Group Project – 1 = (10%)
  - –Class Participation = (5%)

- **Exams (55%)**
  - –Mid Term: 25%
  - –Final Exam: 30%

REDUCTION
EFFECTIVE
DEVELOPMENT
ORGANIZATION
INTERNAL
ASSESSMENT
ASSETS
TRANSFER
THREATS
ACCESS
INTRUSION
SECURITY
AVOIDANCE
CONTROL
EXTERNAL
CLASSIFICATION
MANAGEMENT
DOCUMENTATION
IDENTIFICATION
RISK
IMPLEMENTATION
INFORMATION
POLICY
DETECTION
PROCEDURE


Endpoint Security Management
Reporting & Dashboard
Discovery
Spyware Blocking/ Removal
Inventory
Patch Management
Application Blocking
Connection Control Management
Network Access Control Add-On
Antivirus Add-On
Antivirus Auditing and Enforcement
Audit & Compliance Enforcement
Cloud Services Appliance
Host Intrusion Prevention

SECURITY MANAGEMENT

CHAPTER 1

INTRODUCTION TO SECURITY MANAGEMENT

If this is the information superhighway, it's going through a lot of bad, bad neighborhoods. – Dorian Berger

Contents

- What is Security?, What is Management?
- What is Security Management?
- Principles of information security management
  - Planning, Policy, Programs, Protection, People, Project management
- Project management
- Applying project management to security
- Project management tools

Objectives Chapter 1

1) The importance of the manager's role in securing an organization's use of IT,
2) Understand who is responsible for protecting an organization's information assets
3) Key characteristics of information security
4) Key characteristics of leadership and management
5) Differentiate information security management from general management

Introduction

- **Information Technology (IT)**
  - The vehicle that stores and transports information from one business unit to another
  - The vehicle can break down
- The concept of computer security has been replaced by the concept of information security
  - Covers a broad range of issues
    - From protection of data to protection of human resources

Introduction (cont'd.)

- **Information Security** is no longer the sole responsibility of a discrete group of people in the company
  - – It is the responsibility of every employee, especially managers

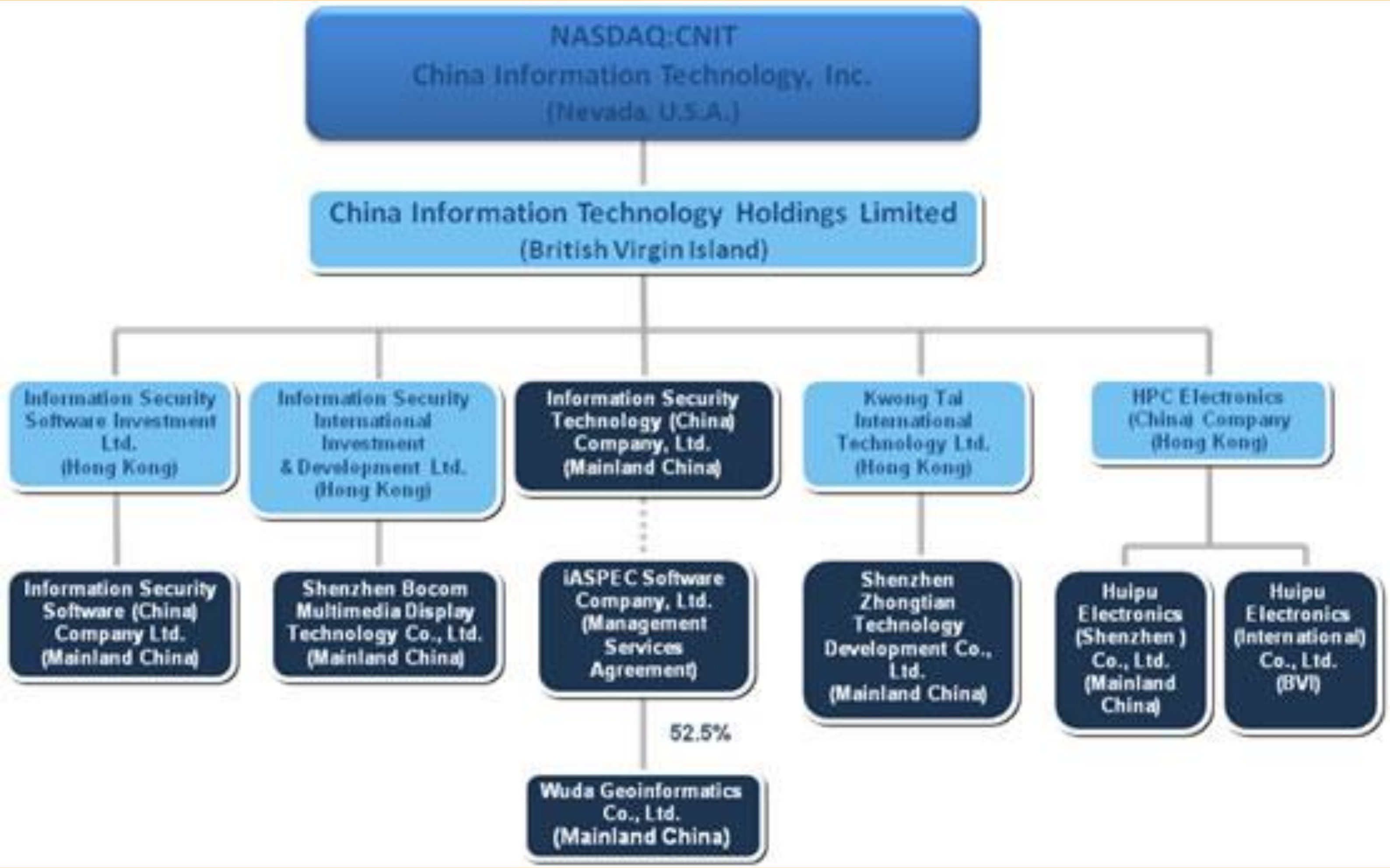
Introduction (cont'd.)

- **Information security decisions** should involve 3 distinct groups of decision makers (communities of interest)
  - Information security managers and professionals
  - Information technology managers and professionals
  - Non-technical business managers and professionals

Introduction (cont'd.)

- **InfoSec community**
  - Protects the organization's information assets from the threats they face.
- **IT community**
  - Supports the business objectives of the organization by supplying and supporting information technology appropriate to the business needs
- **Non-technical general business community**
  - Articulates and communicates organizational policy and objectives and allocates resources to the other groups

Sample 1 organization with IT dep.



NASDAQ:CNIT
China Information Technology, Inc.
(Nevada, U.S.A.)

China Information Technology Holdings Limited
(British Virgin Island)

Information Security Software Investment Ltd.
(Hong Kong)

Information Security International Investment & Development Ltd.
(Hong Kong)

Information Security Technology (China) Company, Ltd.
(Mainland China)

Kwong Tai International Technology Ltd.
(Hong Kong)

HPC Electronics (China) Company
(Hong Kong)

Information Security Software (China) Company Ltd.
(Mainland China)

Shenzhen Bocom Multimedia Display Technology Co., Ltd.
(Mainland China)

iASPEC Software Company, Ltd.
(Management Services Agreement)

Shenzhen Zhongtian Technology Development Co., Ltd.
(Mainland China)

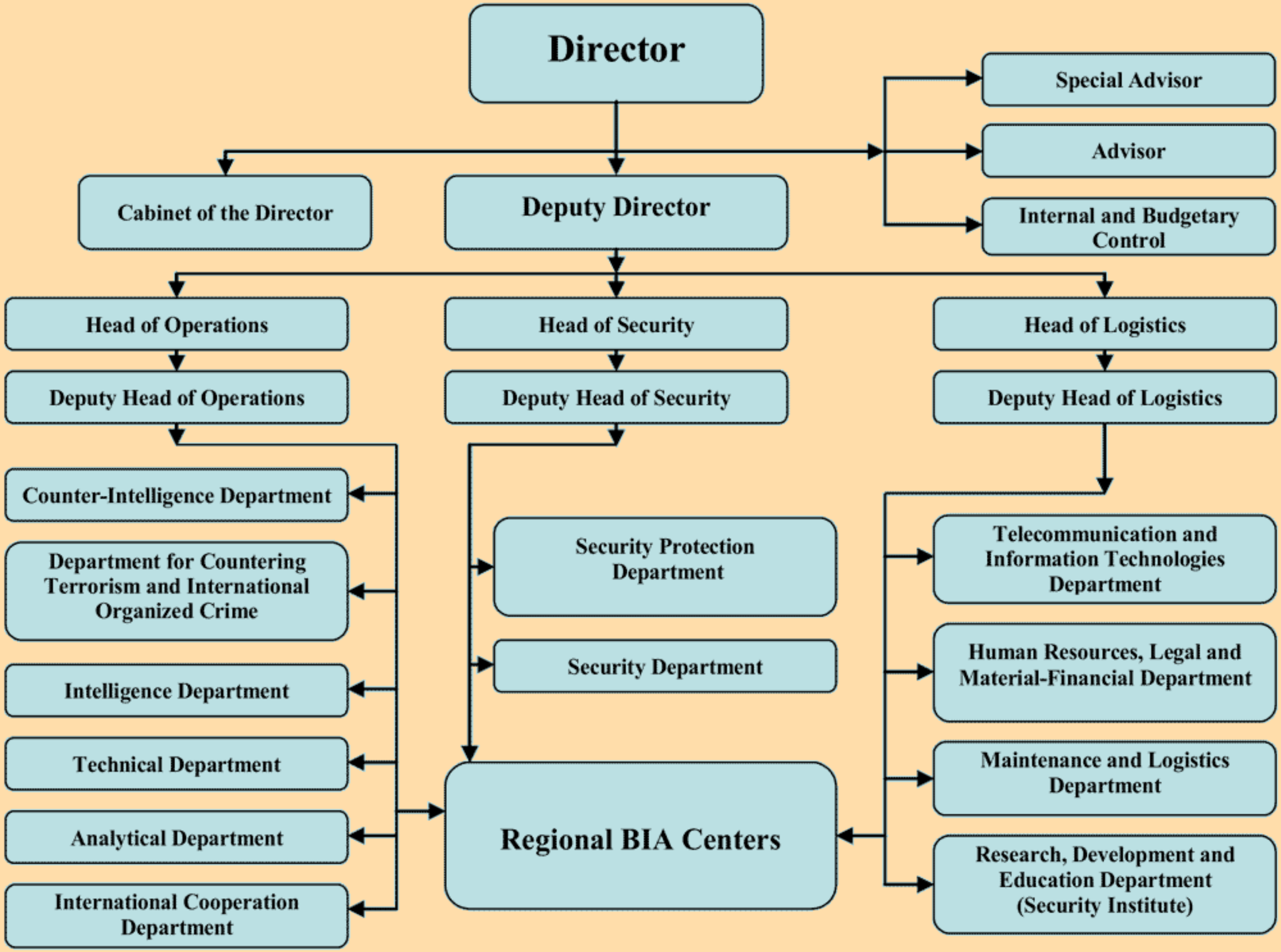
Huipu Electronics (Shenzhen) Co., Ltd.
(Mainland China)

Huipu Electronics (International) Co., Ltd.
(BVI)

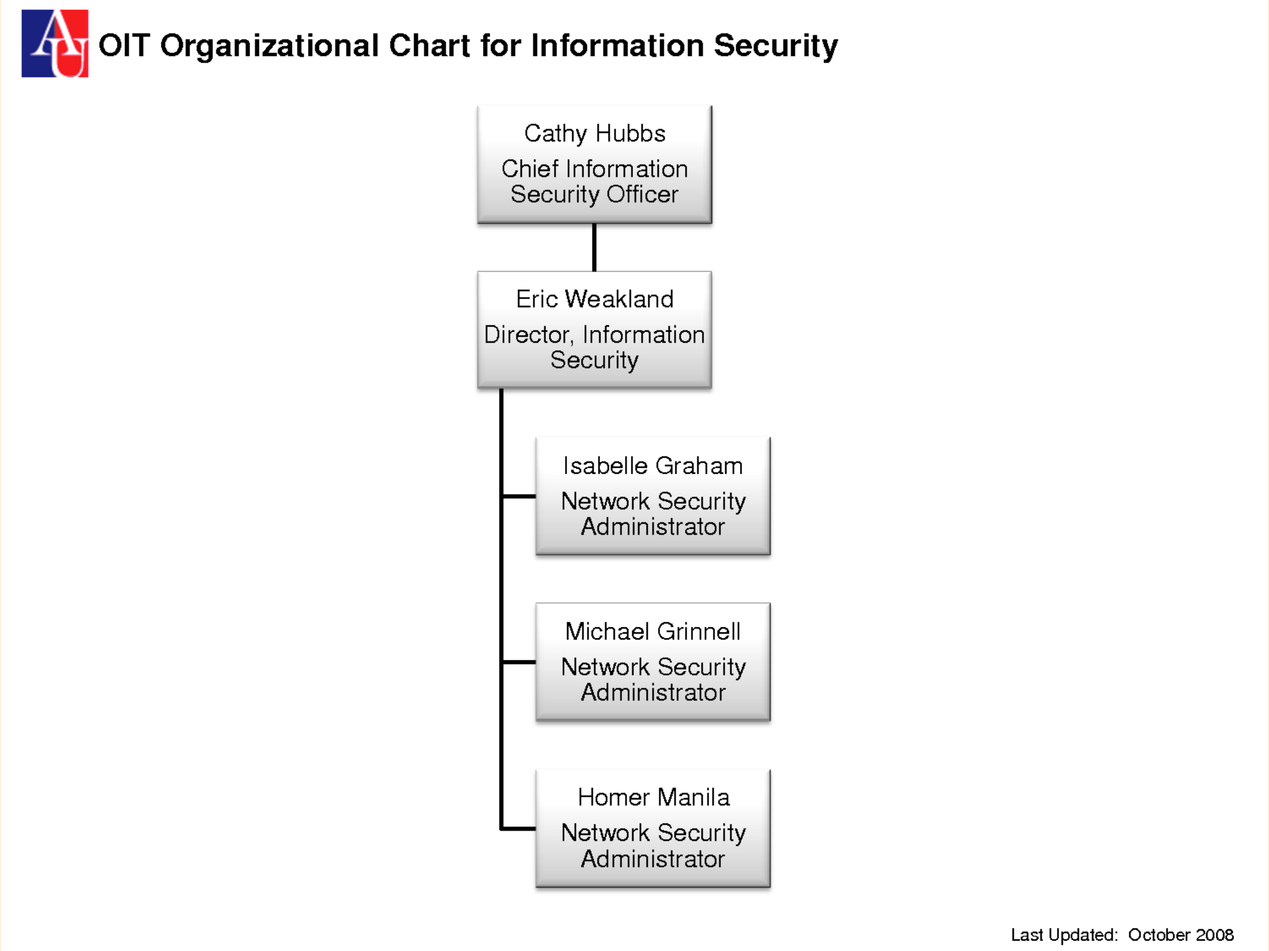
52.5%

Wuda Geoinformatics Co., Ltd.
(Mainland China)

Sample 2 organization with IT dep.


Director
Special Advisor
Advisor
Internal and Budgetary Control
Cabinet of the Director
Deputy Director
Head of Operations
Head of Security
Head of Logistics
Deputy Head of Operations
Deputy Head of Security
Deputy Head of Logistics
Counter-Intelligence Department
Department for Countering Terrorism and International Organized Crime
Intelligence Department
Technical Department
Analytical Department
International Cooperation Department
Security Protection Department
Security Department
Regional BIA Centers
Telecommunication and Information Technologies Department
Human Resources, Legal and Material-Financial Department
Maintenance and Logistics Department
Research, Development and Education Department (Security Institute)

Sample 3 organization with IT dep.



OIT Organizational Chart for Information Security

Cathy Hubbs
Chief Information Security Officer

Eric Weakland
Director, Information Security

Isabelle Graham
Network Security Administrator

Michael Grinnell
Network Security Administrator

Homer Manila
Network Security Administrator

Last Updated: October 2008

What Is Security?

- Definitions
  - **Security** is defined as "**the quality or state of being secure—to be free from danger**"
  - Security is often achieved by means of several strategies undertaken simultaneously or used in combination with one another
- Specialized areas of security
  - Physical security, operations security, communications security, and network security

What Is Security? (cont'd.)

- Information Security
  - – The protection of information and its critical elements (confidentiality, integrity and availability), including the systems and hardware that use, store, and transmit that information
    - Through the application of policy, technology, and training and awareness programs
- Policy, training and awareness programs and technology are vital concepts

CNSS Security Model

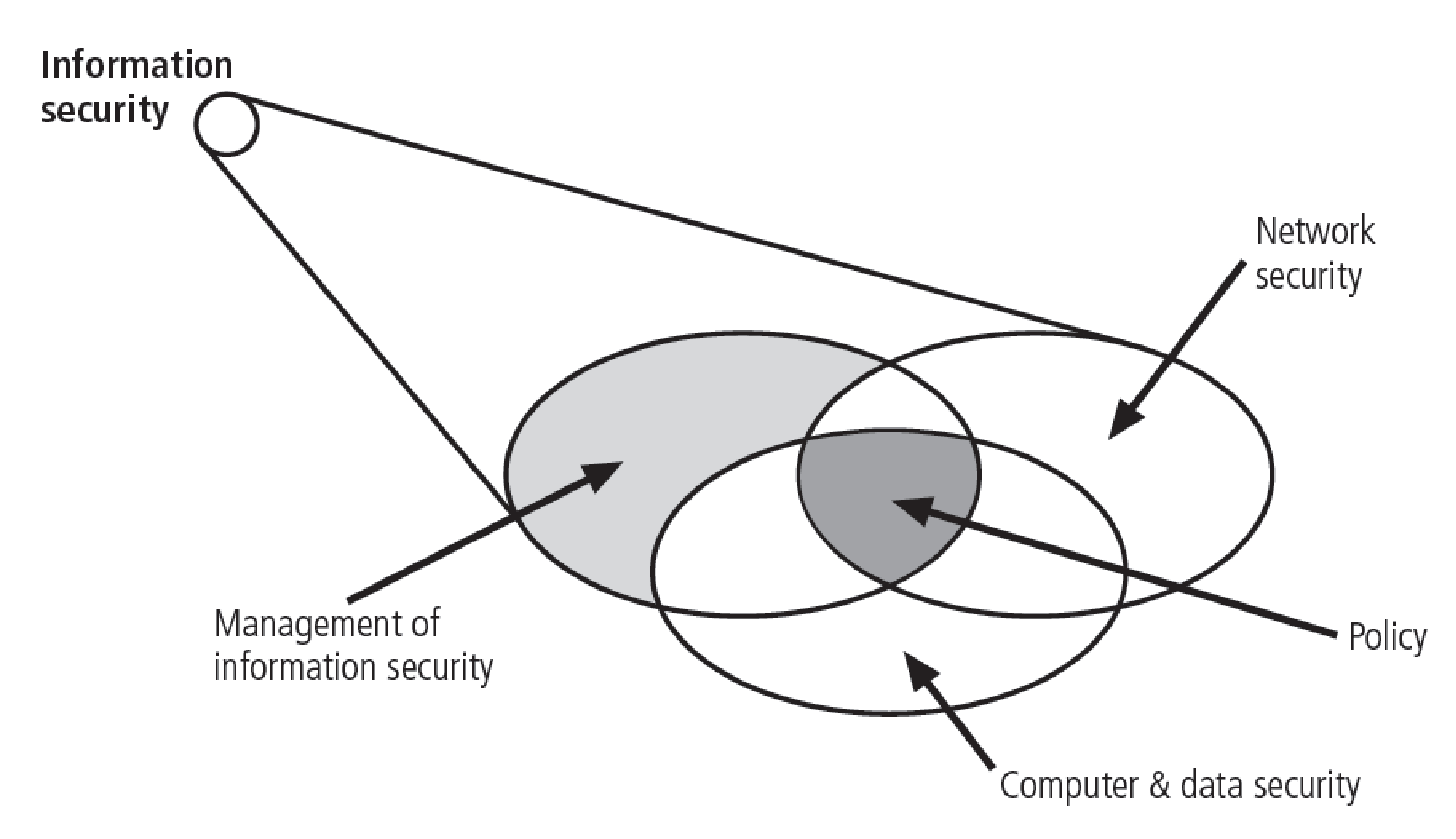


Figure 1-1 Components of Information security

Source: Course Technology/Cengage Learning

** CNSS – Committee on National Security Systems*

CNSS Security Model (cont'd.)

- **C.I.A.** triangle
  - Confidentiality, Integrity, and Availability
  - Has expanded into a more comprehensive list of critical characteristics of information
- **NSTISSC (CNSS) Security Model**
  - Also known as the McCumber Cube
  - Provides a more detailed perspective on security
  - Covers the three dimensions of information security

CNSS Security Model (cont’d.)

- NSTISSC Security Model (cont’d.)
  - Omits discussion of detailed guidelines and policies that direct the implementation of controls
  - Weakness of this model emerges if viewed from a single perspective
    - Need to include all three communities of interest

CNSS Security Model (cont'd.)

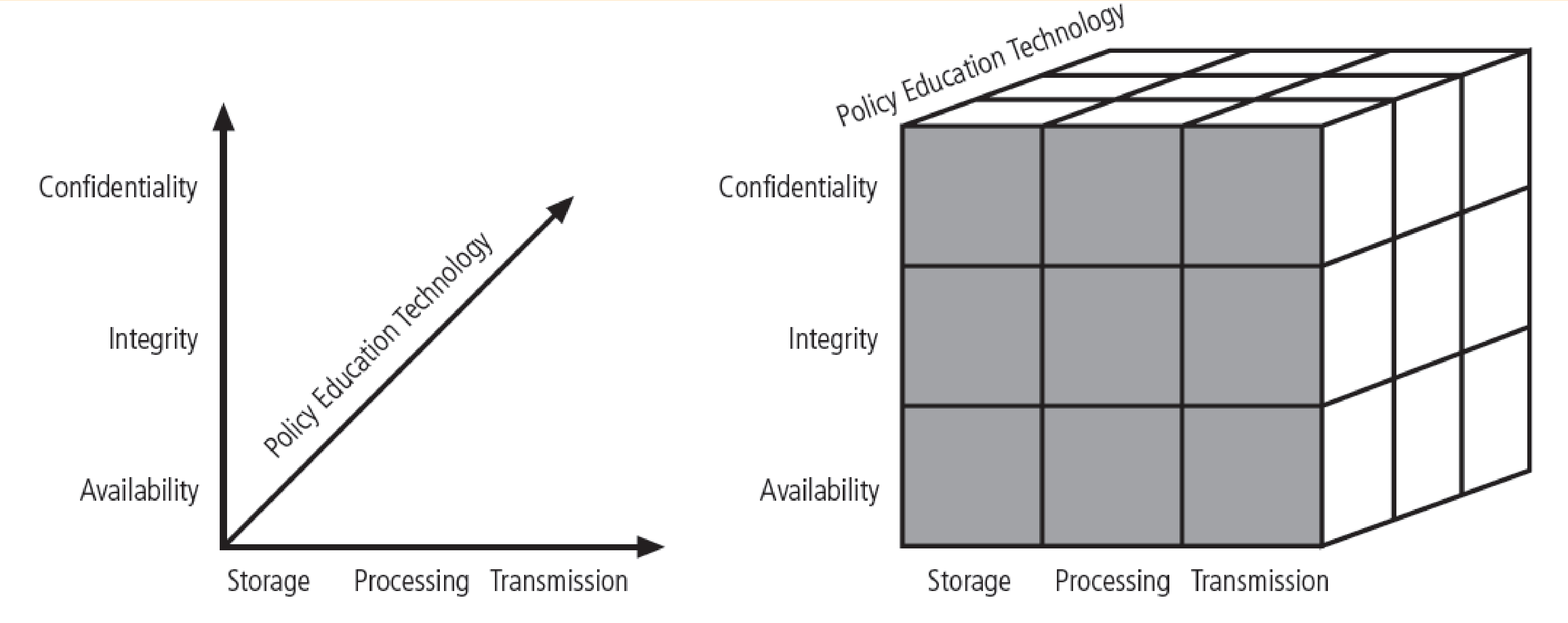


Figure 1-2 CNSS security Model

Source: Course Technology/Cengage Learning
(adapted from NSTISSI No. 4011)

Key Concepts of Information Security (CIA)

- **Confidentiality**
  - The characteristic of information whereby only those with sufficient privileges may access certain information
  - Measures used to protect confidentiality
    - Information classification
    - Secure document storage
    - Application of general security policies
    - Education of information custodians and end users
    - Cryptography

Key Concepts of Information Security (cont'd.)

- **Integrity**
  - – The quality or state of being whole, complete, and uncorrupted
  - – Information integrity is threatened
    - If exposed to corruption, damage, destruction, or other disruption of its authentic state
  - – Corruption can occur while information is being compiled, stored, or transmitted

Key Concepts of Information Security (cont'd.)

- **Availability**
  - – The characteristic of information that enables user access to information in a required format, without interference or obstruction
  - – A user in this definition may be either a person or another computer system
  - – Availability does not imply that the information is accessible to any user
    - Implies availability to authorized users

Key Concepts of Information Security (cont'd.)

- **Privacy**
  - Information collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected
  - Privacy as a characteristic of information does not signify freedom from observation
    - Means that information will be used only in ways known to the person providing it

Key Concepts of Information Security (cont'd.)

- **Identification**
  - An information system possesses the characteristic of identification when it is able to recognize individual users
  - Identification and authentication are essential to establishing the level of access or authorization that an individual is granted

- **Authentication**
  - Occurs when a control proves that a user possesses the identity that he or she claims

Key Concepts of Information Security (cont'd.)

- **Authorization**
  - Assures that the user has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset
  - User may be a person or a computer
  - Authorization occurs after authentication
- **Accountability**
  - Exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process

What Is Management?

- "The process of achieving objectives using a given set of resources"
- Manager
  - – Someone who works with and through other people by coordinating their work activities in order to accomplish organizational goals

What is Management? (cont'd.)

- Managerial roles
  - Informational role
    - Collecting, processing, and using information that can affect the completion of the objective
  - Interpersonal role
    - Interacting with superiors, subordinates, outside stakeholders, and other parties that influence or are influenced by the completion of the task
  - Decisional role
    - Selecting from among alternative approaches, and resolving conflicts, dilemmas, or challenges

What is Management? (cont'd.)

- **Leaders**
  - Influence employees to accomplish objectives
  - Lead by example; demonstrating personal traits that instill a desire in others to follow
  - Provide purpose, direction, and motivation to those that follow
- **Managers**
  - Administers the resources of the organization
  - Creates budgets, authorizes expenditures and hires employees

Behavioral Types of Leaders

- Three basic behavioral types of leaders
  1. **Autocratic**
  2. **Democratic**
  3. **Laissez-faire**

Management Characteristics

- 2 basic approaches to management
  1) **Traditional management theory**
     - Uses the core principles of planning, organizing, *staffing, directing*, and controlling (POSDC)
  2) **Popular management theory**
     - Categorizes the principles of management into planning, organizing, *leading,* and controlling (POLC)

Management Characteristics (cont’d.)

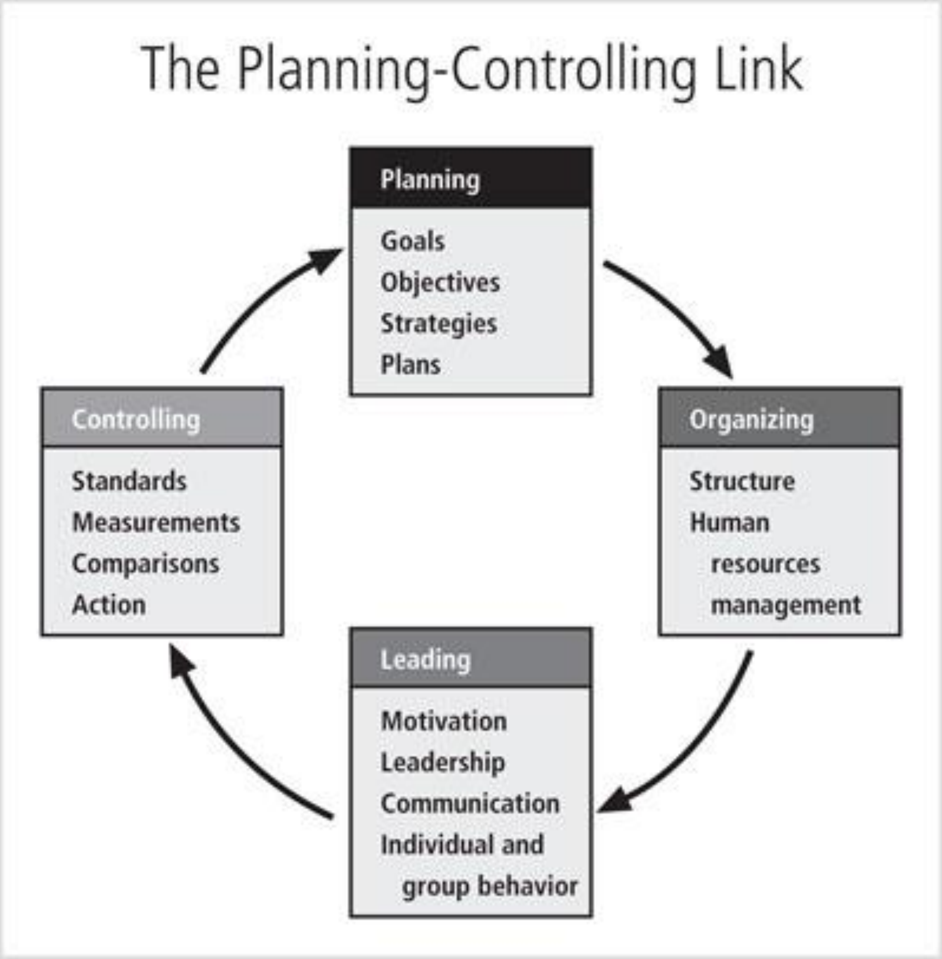


Figure 1-3 The planning-controlling link

Source: Course Technology/Cengage Learning (adapted from Jourdan, 2003)

Management Characteristics (cont’d.)

- **Planning**
  - The process that develops, creates, and implements strategies for the accomplishment of objectives
- 3 levels of Planning

Strategic, Tactical, and Operational

- Planning process begins with the creation of strategic plans for the entire organization

Management Characteristics (cont’d.)

- An organization must thoroughly define its goals and objectives
  - Goals are the end results of the planning process
  - Objectives are intermediate points that allow you to measure progress toward the goal

Management Characteristics (cont’d.)

- **Organizing**
  - The management function dedicated to the structuring of resources to support the accomplishment of objectives
  - Requires determining what is to be done, in what order, by whom, by which methods, and according to what timeline

Management Characteristics (cont'd.)

- **Leading**
  - – Leadership encourages the implementation of the planning and organizing functions
    - Includes supervising employee behavior, performance, attendance, and attitude
  - – Leadership generally addresses the direction and motivation of the human resource

Management Characteristics (cont'd.)

- **Controlling**
  - Monitoring progress toward completion
  - Making necessary adjustments to achieve the desired objectives
  - The control function serves to assure the organization of the validity of the plan
    - Determines what must be monitored as well as applies specific control tools to gather and evaluate information

Management Characteristics (cont'd.)

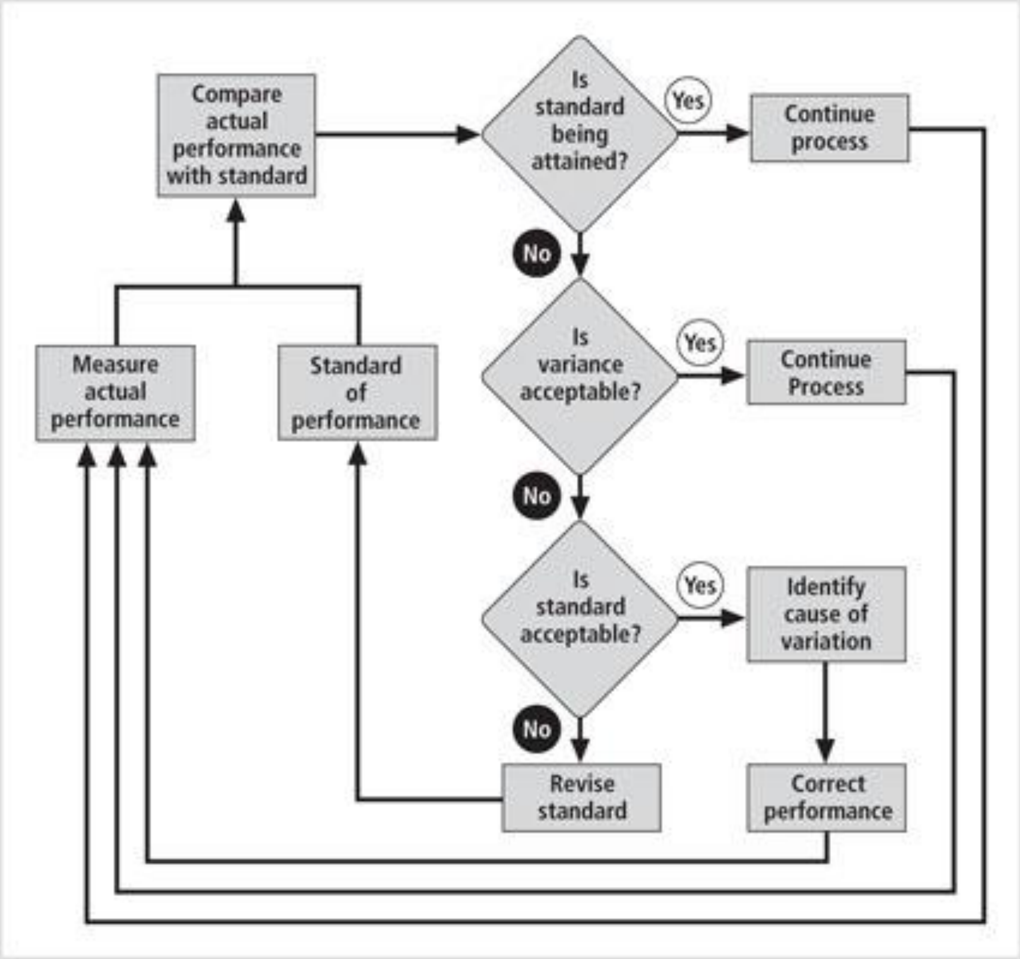


Figure 1-4 The control process

Source: Course Technology/Cengage Learning

Definition of Security Management

"The identification of an organization's assets (including information assets), followed by the development, documentation, and implementation of policies and procedures for protecting these assets"

Solving Problems

- **Step 1**: Recognize and define the problem
- **Step 2**: Gather facts and make assumptions
- **Step 3**: Develop possible solutions
- **Step 4**: Analyze and compare possible solutions
- **Step 5**: Select, implement, and evaluate a solution

Principles of Information Security Management

- The extended characteristics of information security are known as the 6 P’s

1) **Planning**
2) **Policy**
3) **Programs**
4) **Protection**
5) **People**
6) **Project Management**

1. Planning

- Planning as part of InfoSec management
  - An extension of the basic planning model discussed earlier in this chapter
- Included in the InfoSec planning model
  - Activities necessary to support the design, creation, and implementation of information security strategies

1. Planning (cont'd.)

- Types of InfoSec plans
  - Incident response planning
  - Business continuity planning
  - Disaster recovery planning
  - Policy planning
  - Personnel planning
  - Technology rollout planning
  - Risk management planning
  - Security program planning
    - includes education, training and awareness

P2. Policy

- Policy
  - The set of organizational guidelines that dictates certain behavior within the organization
- Three general categories of policy
  - Enterprise information security policy (EISP) – sets tone for InfoSec dep across the organization
  - Issue-specific security policy (ISSP) - acceptable behaviour within a specific techology- email, internet usage
  - System-specific policies (SysSPs) – control the configuration of security equipment – Access Control List (access permitted to the system).

P3. Programs

- Programs
  - InfoSec operations that are specifically managed as separate entities
  - Example: a security education training and awareness (SETA) program
- Other types of programs
  - Physical security program
    - complete with fire, physical access, gates, guards, etc.

P4. Protection

- Executed through risk management activities
  - Including risk assessment and control, protection mechanisms, technologies, and tools
  - Each of these mechanisms represents some aspect of the management of specific controls in the overall information security plan

Risk Management scenario - Database encryption, Data backup failures, Data center access restrictions, Default configurations, threat profiling, Backup media in transit, Single Internet Provider, Assess vulnerability advisories, Identify & rate critical assets, Perform a Risk Assessment of organization in groups

P5. People

- People
  - – The most critical link in the information security program
  - – Managers must recognize the crucial role that people play in the information security program
  - – This area of InfoSec includes security personnel and the security of personnel, as well as aspects of a SETA (security education, training & awareness) program

P6. Project Management

- Project Management
  - Identifying and controlling the resources applied to the project
  - Measuring progress
  - Adjusting the process as progress is made.
  - Project management e.g.:
    - A task to roll out a new security training program
    - To select a new firewall for organization and etc..

Project Management (cont'd.)

- Information security is a **process**, **not** a **project**
  - Each element of an information security program must be managed as a project
  - A continuous series, or chain, of projects
- Some aspects of information security are not project based
  - They are managed processes (operations)

Project Management (cont'd.)

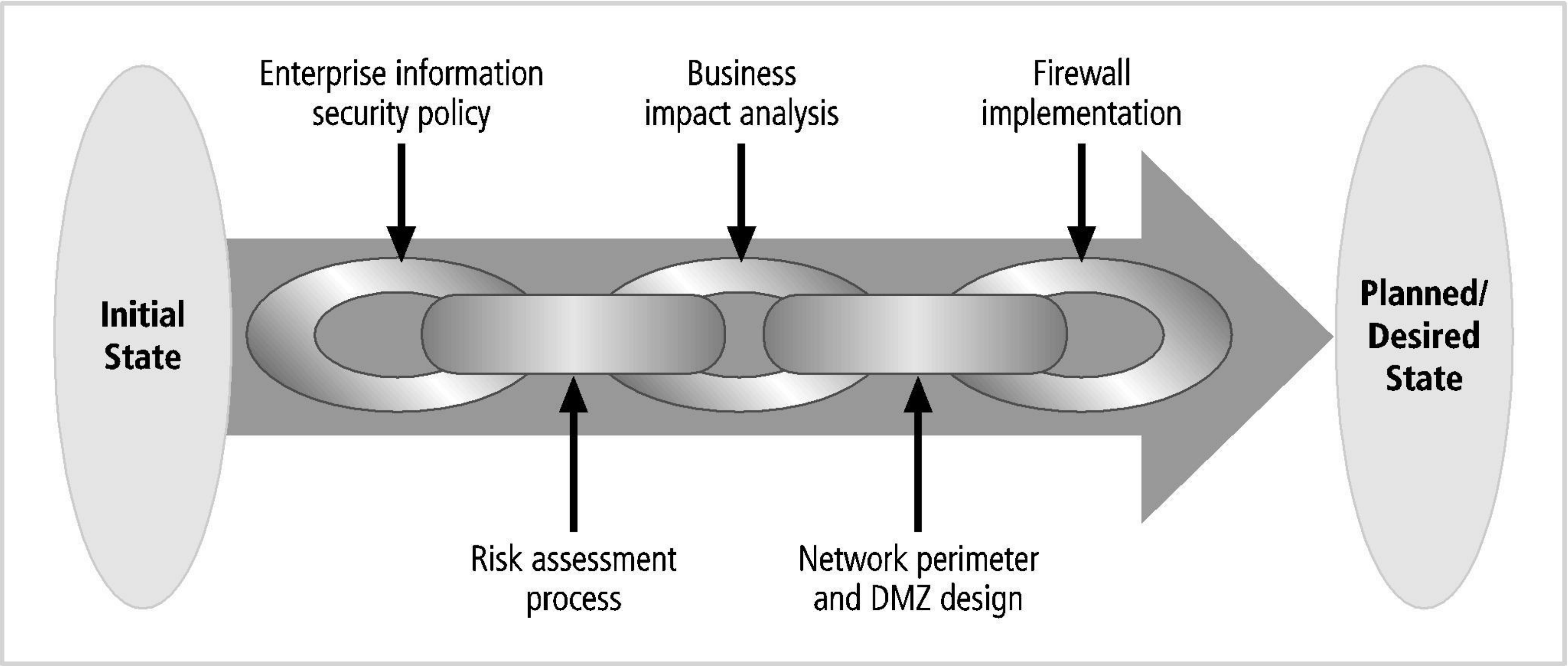


Figure 1-4 The information security program chain

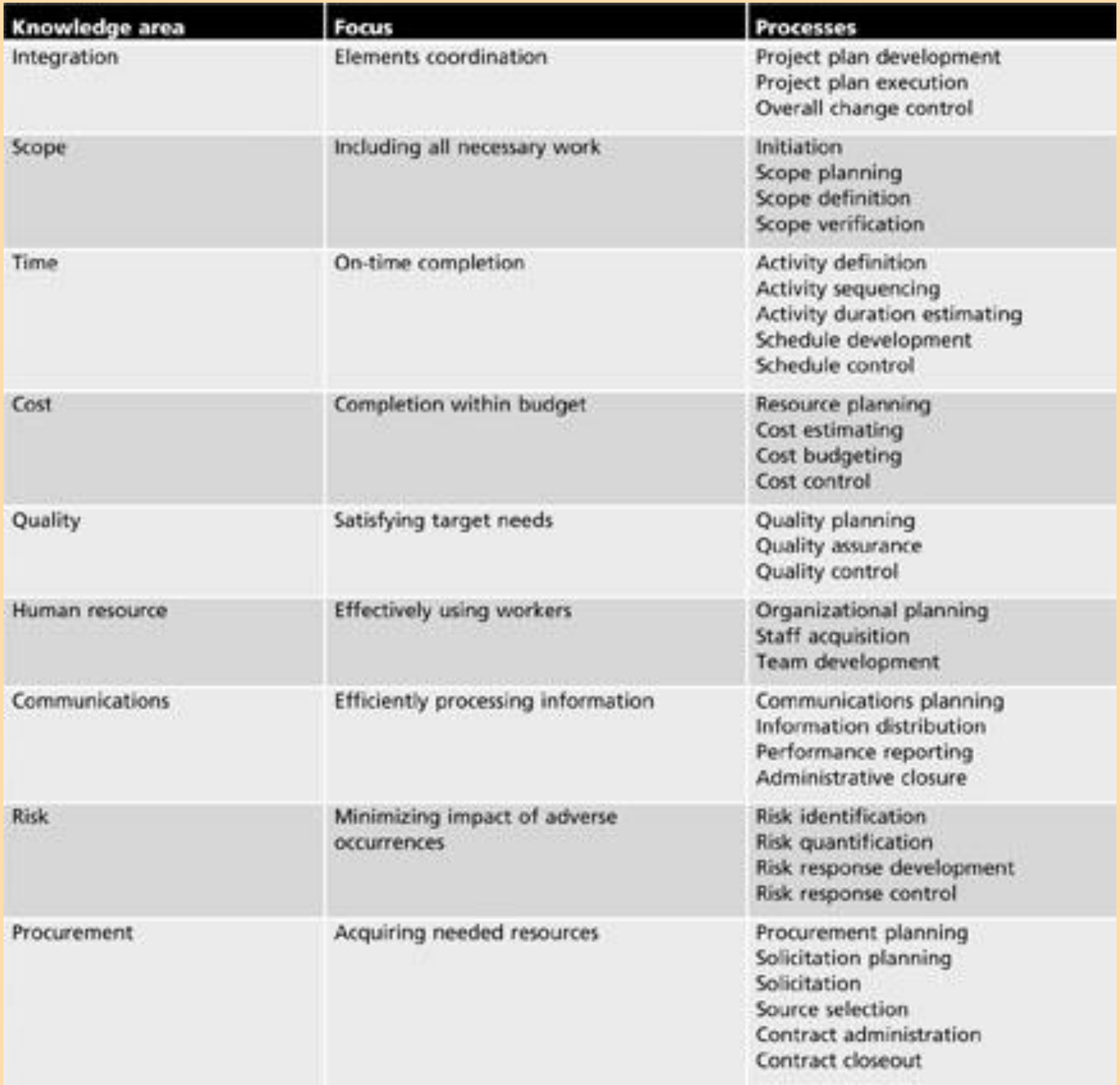
Source: Course Technology/Cengage Learning

Project Management (cont’d.)

- **Project Management**
  - “*The application of knowledge, skills, tools, and techniques to project activities to meet project requirements. Accomplished through the use of processes such as initiating, planning, executing, controlling, and closing.* “ (source the Guide to Project Mgmt Body of Knowledge, W.R. Duncan)
  - Involves the temporary assemblage (collection) resources to complete a project
  - Some projects are iterative, occurring regularly

Applying Project Management to Security

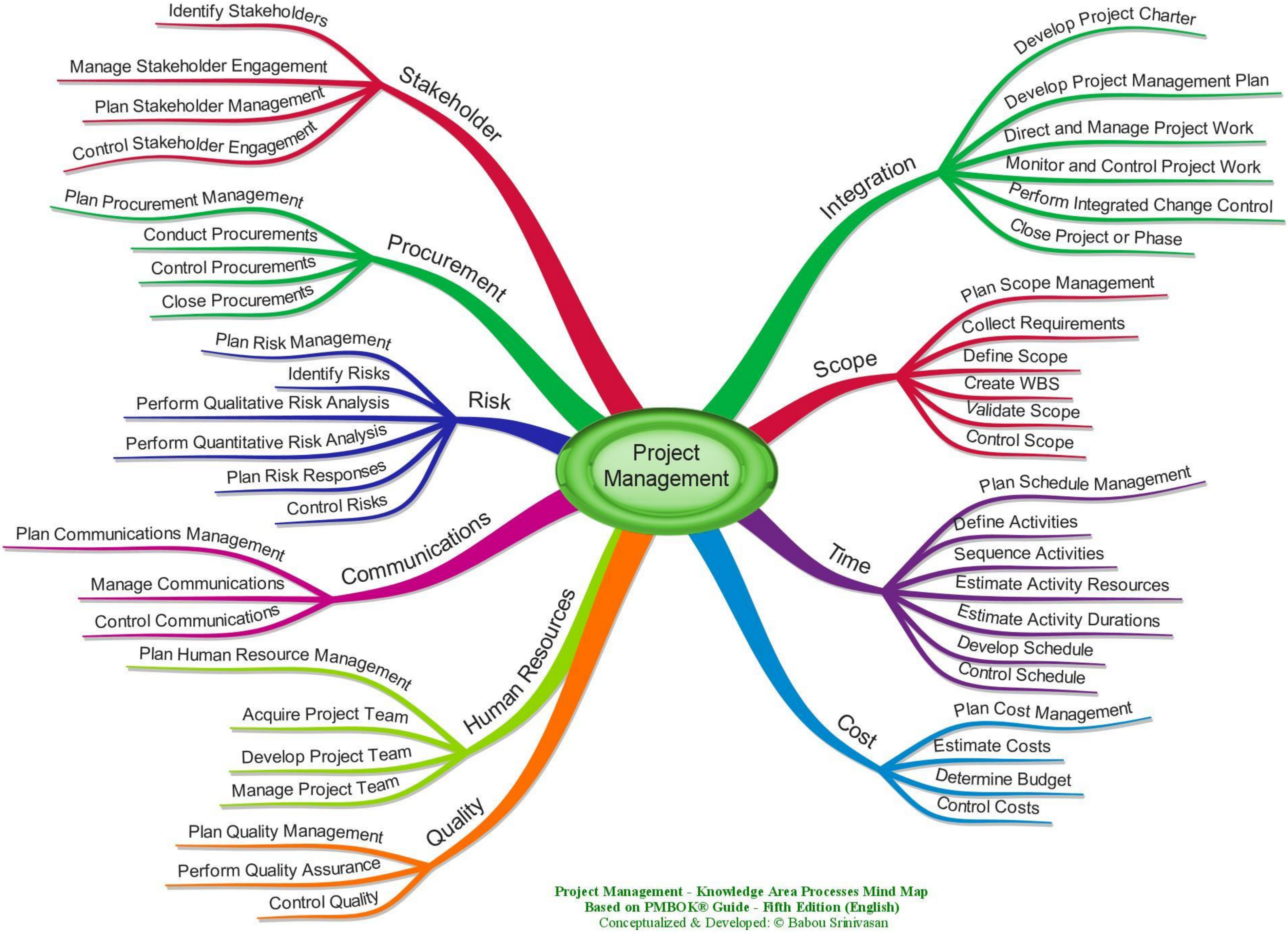
- First identify an established project management methodology (e.g.: SecSDLC)
  - No steps are missed
- ***Project Management Body of Knowledge*** (PMBoK) is considered the industry best practice. Promoted by the *PM Institute*
  - Other project management practices exist



	Knowledge area	Focus	Processes
1	Integration	Elements coordination	Project plan development Project plan execution Overall change control
2	Scope	Including all necessary work	Initiation Scope planning Scope definition Scope verification
3	Time	On-time completion	Activity definition Activity sequencing Activity duration estimating Schedule development Schedule control
4	Cost	Completion within budget	Resource planning Cost estimating Cost budgeting Cost control
5	Quality	Satisfying target needs	Quality planning Quality assurance Quality control
6	Human resource	Effectively using workers	Organizational planning Staff acquisition Team development
7	Communications	Efficiently processing information	Communications planning Information distribution Performance reporting Administrative closure
8	Risk	Minimizing impact of adverse occurrences	Risk identification Risk quantification Risk response development Risk response control
9	Procurement	Acquiring needed resources	Procurement planning Solicitation planning Solicitation Source selection Contract administration Contract closeout

Table 1-1 Project management knowledge areas

Source: Course Technology/Cengage Learning



- Project Management
  - Stakeholder
    - Identify Stakeholders
    - Manage Stakeholder Engagement
    - Plan Stakeholder Management
    - Control Stakeholder Engagement
  - Procurement
    - Plan Procurement Management
    - Conduct Procurements
    - Control Procurements
    - Close Procurements
  - Risk
    - Plan Risk Management
    - Identify Risks
    - Perform Qualitative Risk Analysis
    - Perform Quantitative Risk Analysis
    - Plan Risk Responses
    - Control Risks
  - Communications
    - Plan Communications Management
    - Manage Communications
    - Control Communications
  - Human Resources
    - Plan Human Resource Management
    - Acquire Project Team
    - Develop Project Team
    - Manage Project Team
  - Quality
    - Plan Quality Management
    - Perform Quality Assurance
    - Control Quality
  - Integration
    - Develop Project Charter
    - Develop Project Management Plan
    - Direct and Manage Project Work
    - Monitor and Control Project Work
    - Perform Integrated Change Control
    - Close Project or Phase
  - Scope
    - Plan Scope Management
    - Collect Requirements
    - Define Scope
    - Create WBS
    - Validate Scope
    - Control Scope
  - Time
    - Plan Schedule Management
    - Define Activities
    - Sequence Activities
    - Estimate Activity Resources
    - Estimate Activity Durations
    - Develop Schedule
    - Control Schedule
  - Cost
    - Plan Cost Management
    - Estimate Costs
    - Determine Budget
    - Control Costs

Project Management - Knowledge Area Processes Mind Map
Based on PMBOK® Guide - Fifth Edition (English)
Conceptualized & Developed: © Babou Srinivasan

PMBoK Knowledge Areas

Area 1: Project Integration Management

- Includes the processes required to coordinate occurs between components of a project (e.g.: financial resources, internal coordination units, computing resource, physical resource (meeting room) etc..

- Major Elements of a project management effort that require integration
  - The development of the initial project plan
  - Monitoring of progress during plan execution
  - Control of plan revisions

PMBoK Knowledge Areas (cont'd.)

- Elements of a project management effort that require integration (cont'd.)
  - Control of the changes made to resource allocations
    - As measured performance causes adjustments to the project plan

PMBoK Knowledge Areas (cont'd.)

- Project Plan Development
  - The process of integrating all of the project elements into a cohesive plan
    - Goal is to complete the project within the allotted work time using no more than the allotted project resources
- Core components of project plan
  - **Work time, resources,** and **project deliverables**
  - Changing one element affects the other two
    - Likely requires revision of the plan

PMBoK Knowledge Areas (cont'd.)

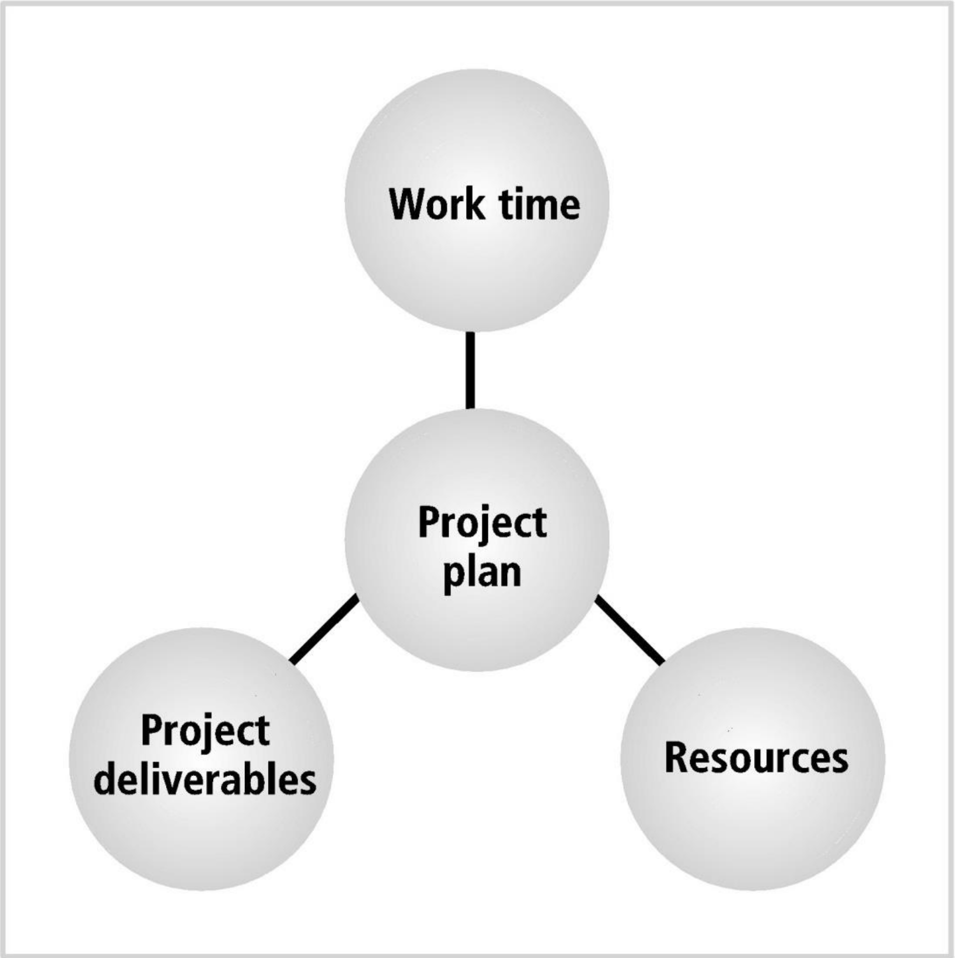


Figure 1-7 Project plan inputs

Source: Course Technology/Cengage Learning

PMBoK Knowledge Areas (cont'd.)

- When integrating the disparate/different elements of a complex information security project, complications are likely to arise
  - Conflicts among communities of interest
  - Far-reaching impact
  - Resistance to new technology

PMBoK Knowledge Areas (cont'd.)

Area 2: Project Scope Management

- Ensures that project plan includes only those activities necessary to complete it

- Scope
  - The quantity or quality of project deliverables
- Major processes
  - Initiation, scope planning, definition, verification and change control

PMBoK Knowledge Areas (cont'd.)

Area 3: Project Time Management

- Ensures that project is finished by identified completion date while meeting objectives
- Failure to meet project deadlines is among most frequently cited failures in project management
  - Many missed deadlines are caused by **poor planning**

PMBoK Knowledge Areas (cont'd.)

- Project time management includes the following processes
    i. Activity definition
    ii. Activity sequencing
    iii. Activity duration estimating
    iv. Schedule development
    v. Schedule control

PMBoK Knowledge Areas (cont'd.)

Area 4: Project Cost Management

- Ensures that a project is completed within the resource constraints
- Some projects are planned using only a financial budget
    - From which all resources must be procured
- Includes resource planning, cost estimating, cost budgeting, and cost control

PMBoK Knowledge Areas (cont'd.)

Area 5: Project Quality Management

- Ensures project meets project specifications
- Quality objective met
  - When deliverables meet requirements specified in project plan
- A good plan defines project deliverables in unambiguous terms
  - For easy comparison against actual results
- Includes quality planning, quality assurance and quality control

PMBoK Knowledge Areas (cont'd.)

Area 6: Project Human Resource Management

- Ensures personnel assigned to project are effectively employed
- Staffing a project requires careful estimates of effort required
- Unique complexities
  - Extended clearances
  - Deploying technology new to the organization
- Includes organizational planning, staff acquisition and team development

PMBoK Knowledge Areas (cont'd.)

Area 7: Project Communications Management

- Conveys details of project activities to all involved
- Includes the creation, distribution, classification, storage, and destruction of documents, messages, and other associated project information
- Includes communications planning, information distribution, performance reporting and administrative closure

PMBoK Knowledge Areas (cont'd.)

Area 8: Project Risk Management

- Assesses, mitigates, manages, and reduces the impact of adverse occurrences on the project
- Information security projects have unique risks
- Includes risk identification, risk quantification, risk response development and risk response control

PMBoK Knowledge Areas (cont'd.)

Area 9: Project Procurement

- Acquiring needed project resources
- Project managers may simply requisition resources from organization, or may have to purchase
- Includes procurement planning, solicitation planning, solicitation, source selection, contract administration and contract closeout
- E.g.: project to need different software or hardware, different skilled human resource

Project Management Tools

- Many tools exist (e.g.: PERT – program evaluation review technique, CPM – critical path method)
  - Most project managers combine software tools that implement one or more of the dominant modeling approaches
- Project management certification
  - The Project Management Institute (PMI)
    - Leading global professional association
    - Sponsors two certificate programs: The Project Management Professional (PMP) and Certified Associate in Project Management (CAPM)

Project Management Tools (cont'd.)

- **Projectitis** (InfoSec complication)
  - Occurs when the project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts than accomplishing meaningful project work.
- Precursor to projectitis
  - Developing an overly elegant, microscopically detailed plan before gaining consensus for the work required – proper use project tools can help

Work Breakdown Structure

- **Work Breakdown Structure (WBS)**
  - Simple planning tool for creating a project plan
  - The project plan is first broken down into a few major tasks
    - Each task is placed on the WBS task list

Work Breakdown Structure (cont'd.)

- Determine minimum attributes for each task
  - The work to be accomplished (activities and deliverables)
  - Estimated amount of effort required for completion in hours or workdays
  - The common or specialty skills needed to perform the task
  - Task interdependencies

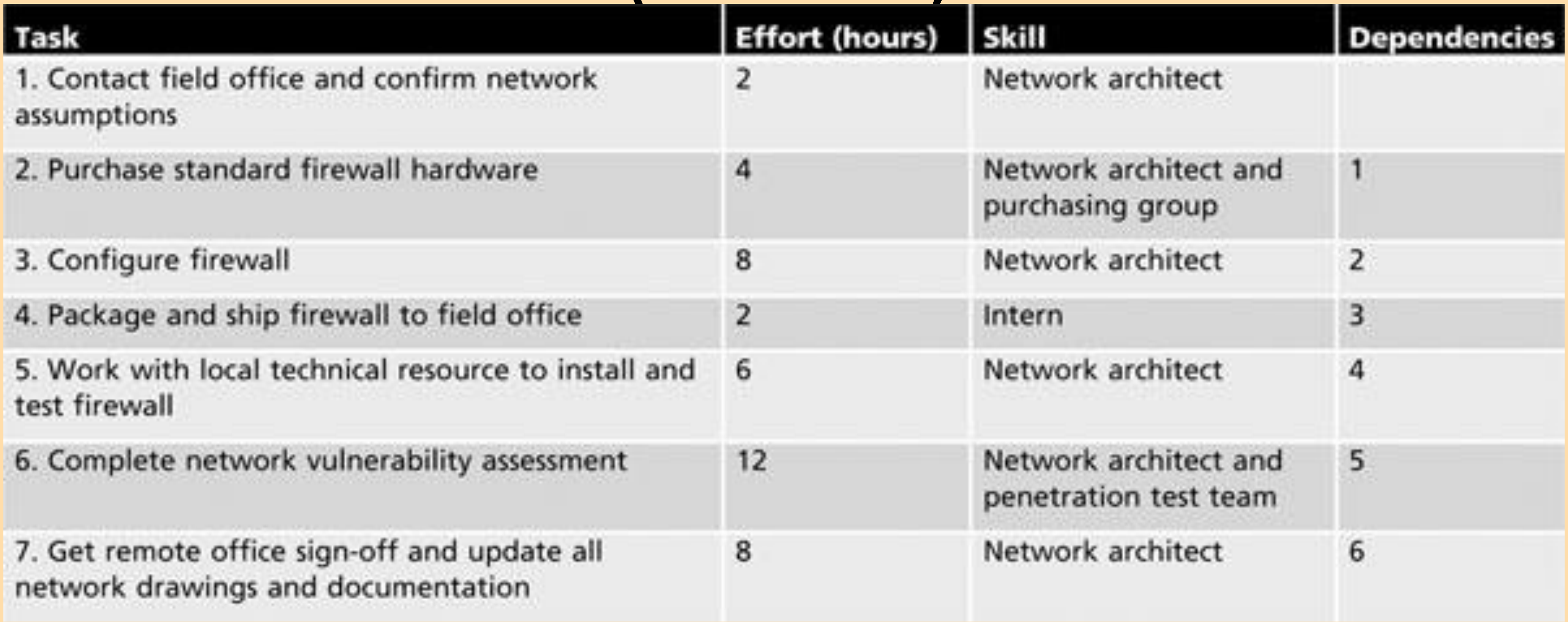
Work Breakdown Structure (cont’d.)

- As the project plan develops, additional attributes can be added
  - ✓ Estimated capital and noncapital expenses for the task
  - ✓ Task assignment according to specific skills
  - ✓ Start and end dates
  - ✓ Work to be accomplished
  - ✓ Amount of effort
  - ✓ Task dependencies
  - ✓ Start and ending dates

Work Breakdown Structure (cont'd.)

- Work phase
  - Phase in which the project deliverables are prepared
  - Occurs after the project manager has completed the WBS

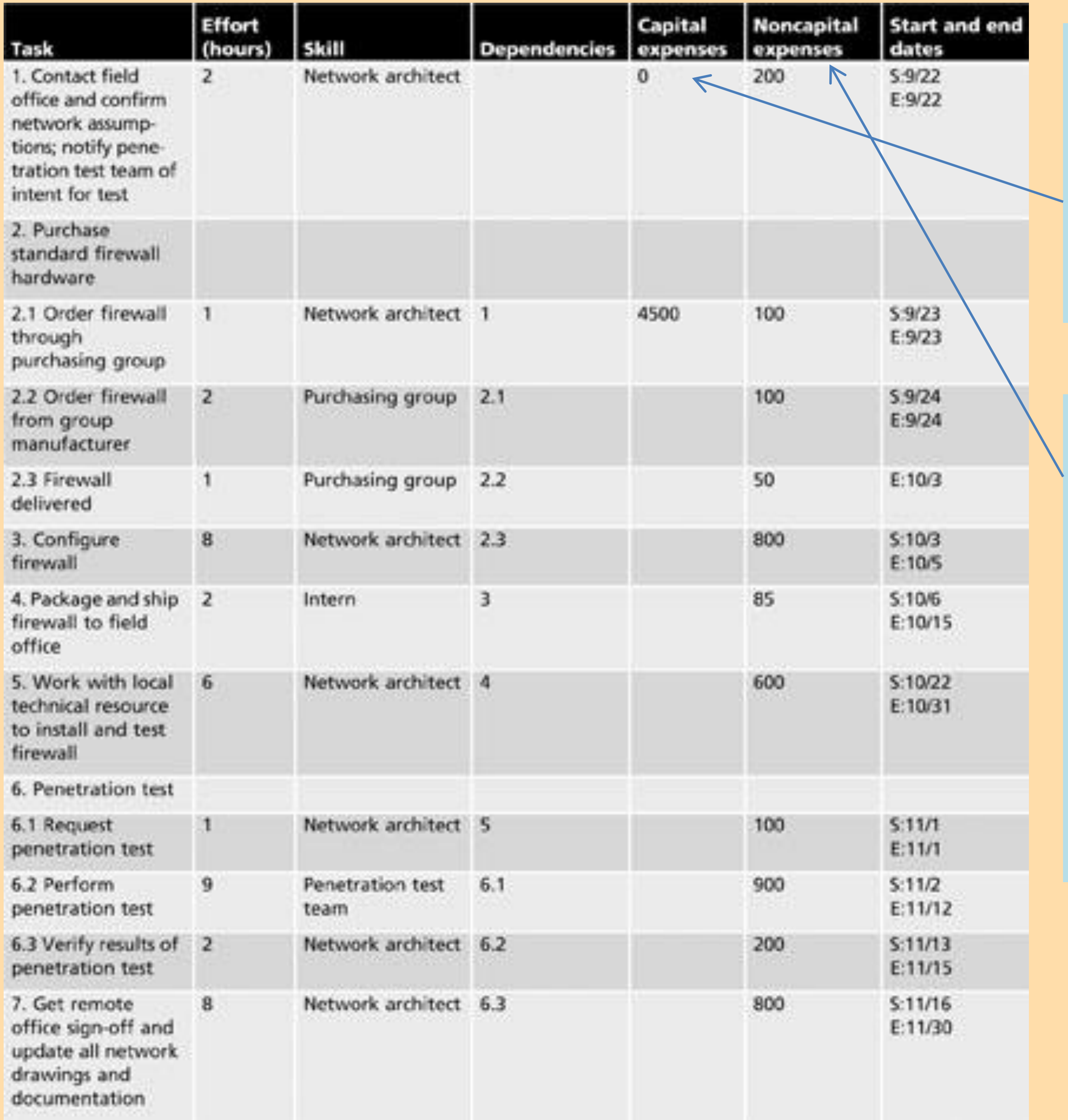
Work Breakdown Structure (cont'd.)



Task	Effort (hours)	Skill	Dependencies
1. Contact field office and confirm network assumptions	2	Network architect	
2. Purchase standard firewall hardware	4	Network architect and purchasing group	1
3. Configure firewall	8	Network architect	2
4. Package and ship firewall to field office	2	Intern	3
5. Work with local technical resource to install and test firewall	6	Network architect	4
6. Complete network vulnerability assessment	12	Network architect and penetration test team	5
7. Get remote office sign-off and update all network drawings and documentation	8	Network architect	6

Table 1-2 Early draft work breakdown structure

Source: Course Technology/Cengage Learning



Task	Effort (hours)	Skill	Dependencies	Capital expenses	Noncapital expenses	Start and end dates
1. Contact field office and confirm network assumptions; notify penetration test team of intent for test	2	Network architect		0	200	S:9/22 E:9/22
2. Purchase standard firewall hardware						
2.1 Order firewall through purchasing group	1	Network architect	1	4500	100	S:9/23 E:9/23
2.2 Order firewall from group manufacturer	2	Purchasing group	2.1		100	S:9/24 E:9/24
2.3 Firewall delivered	1	Purchasing group	2.2		50	E:10/3
3. Configure firewall	8	Network architect	2.3		800	S:10/3 E:10/5
4. Package and ship firewall to field office	2	Intern	3		85	S:10/6 E:10/15
5. Work with local technical resource to install and test firewall	6	Network architect	4		600	S:10/22 E:10/31
6. Penetration test						
6.1 Request penetration test	1	Network architect	5		100	S:11/1 E:11/1
6.2 Perform penetration test	9	Penetration test team	6.1		900	S:11/2 E:11/12
6.3 Verify results of penetration test	2	Network architect	6.2		200	S:11/13 E:11/15
7. Get remote office sign-off and update all network drawings and documentation	8	Network architect	6.3		800	S:11/16 E:11/30

Table 1-3 Later draft work breakdown structure

Source: Course Technology/Cengage Learning

Capital Expenses - payments by a business for fixed assets

Non-capital Expenses – expenditure spent on repairs, supplies, payroll, and other operating expenses.

Task-Sequencing Approaches

- Many possibilities for task assignment and scheduling
  - For modest and large size projects
- A number of approaches can assist the project manager in this sequencing effort
  - Network scheduling
    - Refers to the web of possible pathways to project completion

Network here doesn't refer to computer network

Task Sequencing Approaches (cont'd.)

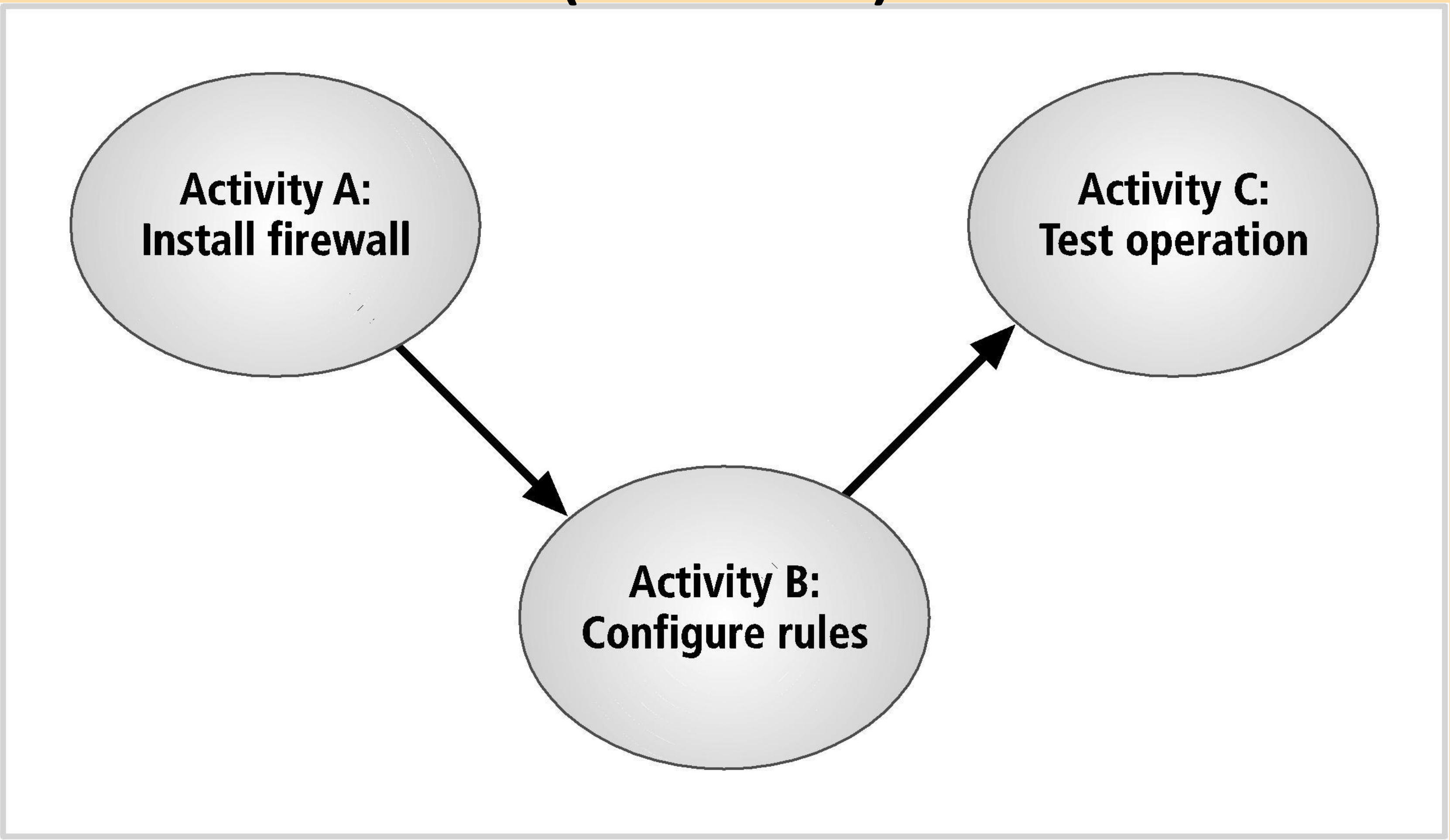


Figure 1-8 Simple network dependency

Source: Course Technology/Cengage Learning

Task Sequencing Approaches (cont'd.)

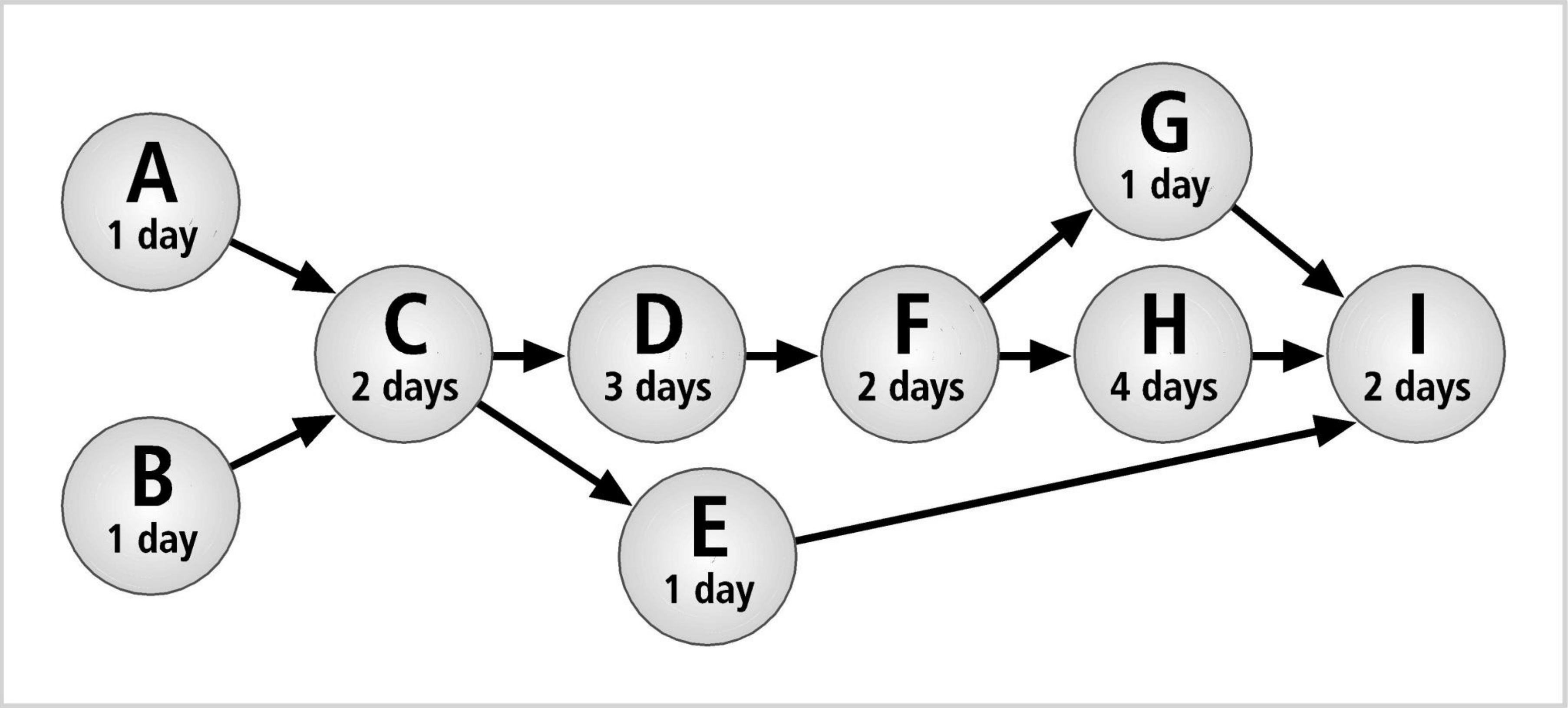


Figure 1-9 Complex network dependency

Source: Course Technology/Cengage Learning

Task Sequencing Approaches (cont'd.)

- **Program Evaluation and Review Technique (PERT)**
  - Most popular technique
  - Originally developed in the late 1950's for government-driven engineering projects

Task Sequencing Approaches (cont'd.)

- 3 key questions
  - – How long will this activity take?
  - – What activity occurs immediately before this activity can take place?
  - – What activity occurs immediately after this activity?
- Determine the critical path
  - – By identifying the slowest path through the various activities

Task Sequencing Approaches (cont'd.)

- Slack time
  - How much time is available for starting a non-critical task without delaying the project as a whole
  - Tasks which have slack time are logical candidates for accepting a delay

Task Sequencing Approaches (cont'd.)

- PERT advantages
  - Makes planning large projects easier
    - By facilitating the identification of pre- and post-activities
  - Determines the probability of meeting requirements
  - Anticipates the impact of system changes
  - Presents information in a straightforward format understood by managers
    - Requires no formal training

Task Sequencing Approaches (cont’d.)

- PERT disadvantages
  - Diagrams can be awkward and cumbersome, especially in very large projects
  - Diagrams can become expensive to develop and maintain
    - Due to the complexities of some project development processes
  - Difficulty in estimating task durations
    - Inaccurate estimates invalidate any close critical path calculations

Task Sequencing Approaches (cont'd.)

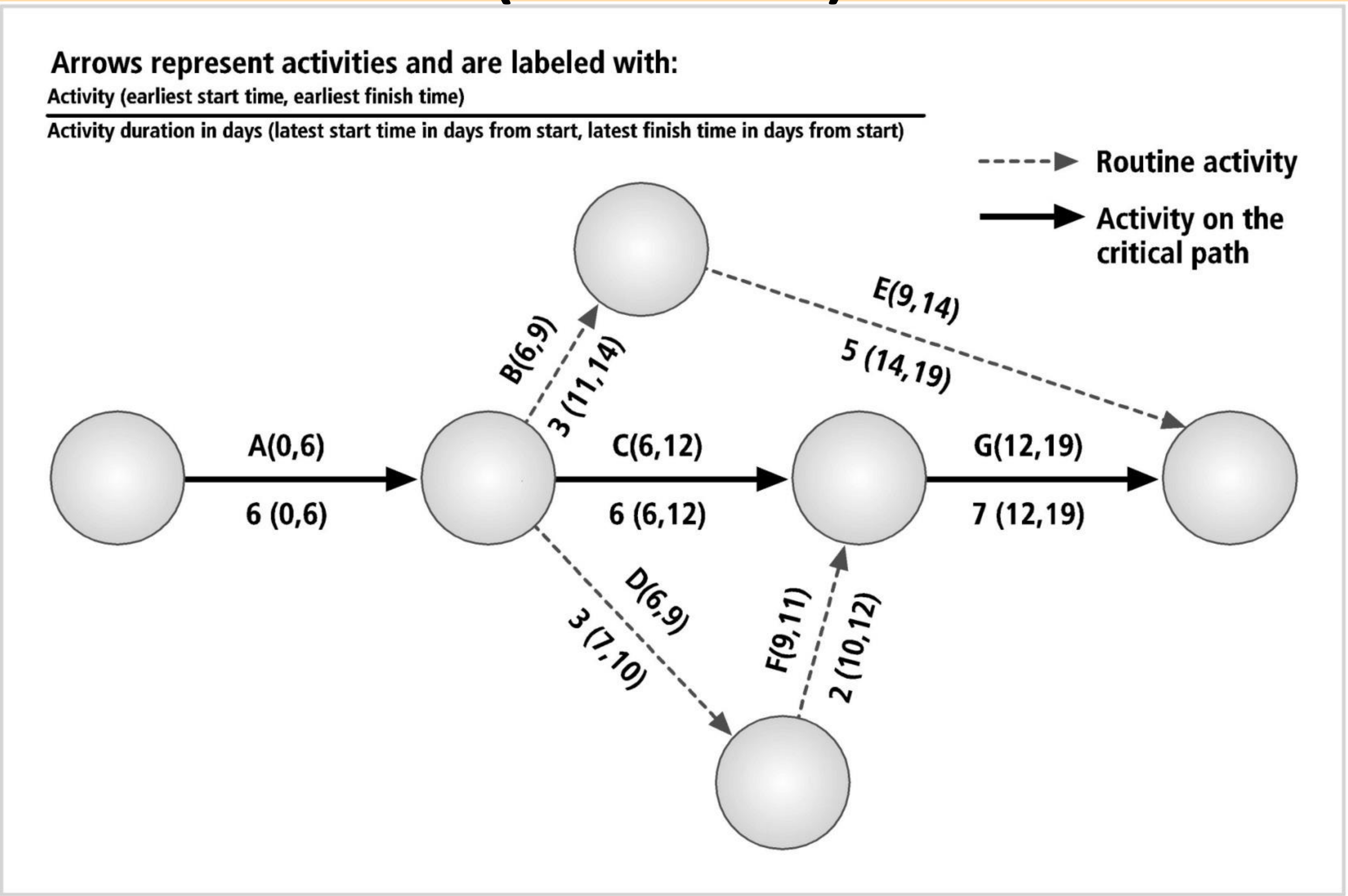

Arrows represent activities and are labeled with:
Activity (earliest start time, earliest finish time)
Activity duration in days (latest start time in days from start, latest finish time in days from start)
Routine activity
Activity on the critical path
A(0,6)
6 (0,6)
B(6,9)
3 (11,14)
C(6,12)
6 (6,12)
D(6,9)
3 (7,10)
E(9,14)
5 (14,19)
F(9,11)
2 (10,12)
G(12,19)
7 (12,19)

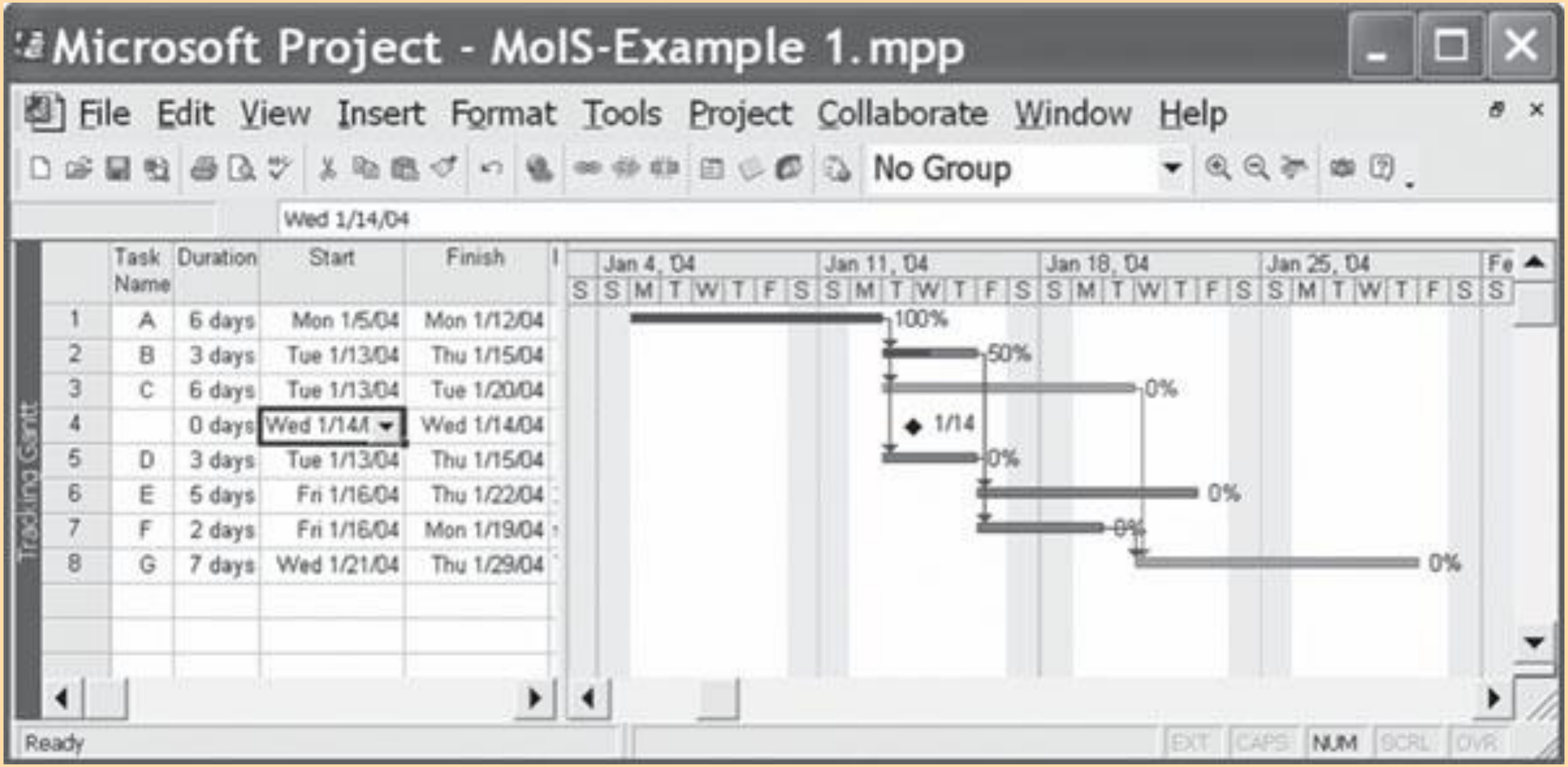
Figure 1-10 PERT example

Source: Course Technology/Cengage Learning

Task Sequencing Approaches (cont'd.)

- **Gantt Chart**
  - Easy to read and understand; easy to present to management
  - Easier to design and implement than the PERT diagrams, yielding much of the same information
  - Lists activities on the vertical axis of a bar chart, and provides a simple time line on the horizontal axis

Task Sequencing Approaches (cont'd.)



Microsoft Project - MoIS-Example 1.mpp

	Task Name	Duration	Start	Finish
1	A	6 days	Mon 1/5/04	Mon 1/12/04
2	B	3 days	Tue 1/13/04	Thu 1/15/04
3	C	6 days	Tue 1/13/04	Tue 1/20/04
4		0 days	Wed 1/14/(	Wed 1/14/04
5	D	3 days	Tue 1/13/04	Thu 1/15/04
6	E	5 days	Fri 1/16/04	Thu 1/22/04
7	F	2 days	Fri 1/16/04	Mon 1/19/04
8	G	7 days	Wed 1/21/04	Thu 1/29/04

Figure 1-11 Project Gantt chart

Source: Course Technology/Cengage Learning

Automated Project Tools

- **Microsoft Project**
  - – A widely used project management tool
- Keep in mind:
  - – A software program is no substitute for a skilled and experienced project manager
    - Manager must understand how to define tasks, allocate scarce resources, and manage assigned resources
  - – A software tool can get in the way of the work
  - – Choose a tool that you can use effectively

Summary

- What is Security?
- What is Management?
- Principles of information security management
  - Planning, Policy, Programs, Protection, People, Project management
- Project management
- Applying project management to security
- Project management tools