Information Systems Security

Lectures 10, 11, 12

Information Security Management

Dr. En. Bader Ahmad

References

1. James Joshi, Security Management Course, http://www.sis.pitt.edu/~jjoshi/IS2820/Fall2007

2. *Network security, The complete Reference*. R. Bragg, M. Rhodes-Ousley, K. Strassberg. McGraw-Hill Osborne, 2004.

3. Management of Information Security, M. E. Whitman, H. J. Mattord

Objective

- The course is aimed at imparting knowledge and skill sets required to assume the overall responsibilities of administration and management of security of an enterprise information system.

Learning Outcome

- After the course, ability to carry out:
  - Detailed analysis of enterprise security by performing various types of analysis
  - Carry out the task of security risk management using various tools.
  - Design detailed enterprise wide security plans and policies, and deploy appropriate safeguards (models, mechanisms and tools)

Outline

1. Introduction
2. Security Planning
3. Continuity Planning
4. Policy
5. Security Management Models and Practices
6. Risk Management
7. Legal and Ethics Issues

Information Security Management

1. Introduction

Outline

1. Introduction
2. Characteristics of management
3. Principles of Information Security Management

1. Introduction

- Information technology is critical to business and society

- Information Security protects:
  - Data
  - Human resources
  - …

- Information security is the responsibility of every member of an organization, especially managers.

Introduction

- Information security involves three decision makers:
  - Information security managers and professionals
  - Information technology managers and professionals
  - Non-technical business managers and professionals
- Communities roles:
  - InfoSec community:
    - protect information assets from threats
  - IT community:
    - support business objectives by supplying appropriate information technology
  - Business community:
    - policy and resources

What Is Security?

- **Security** is "The quality or state of being secure—to be free from danger"

- Security is often achieved by means of several strategies usually undertaken simultaneously or used in combination with one another:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security

What Is Management?

- **Management** : process of achieving objectives using a given set of resources.

- To manage the information security process, first understand core principles of management.

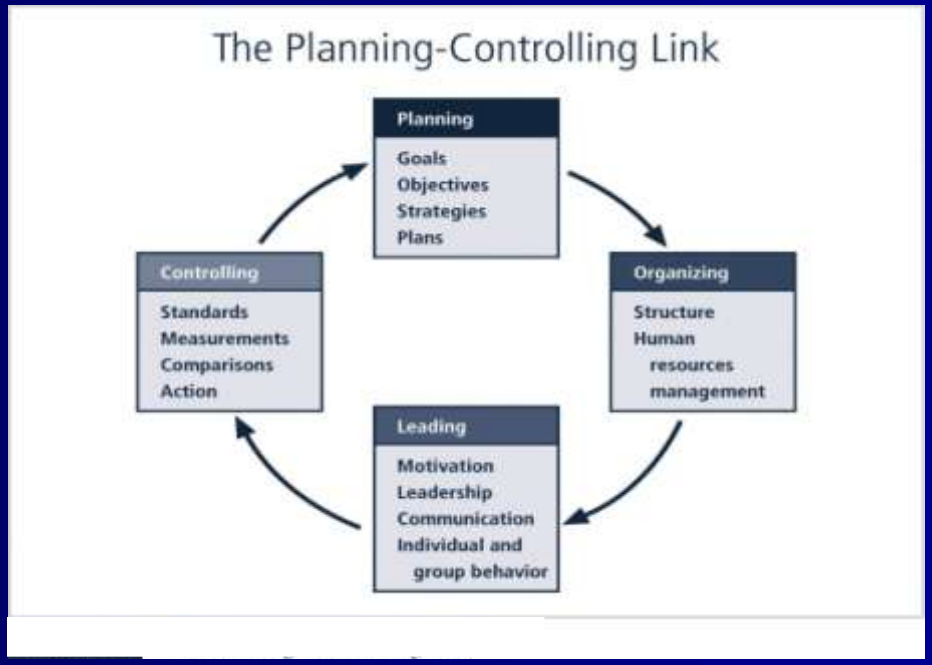
- A manager is
  - "someone who works with and through other people by coordinating their work activities in order to accomplish organizational goals".

Managerial Roles

- Informational role: Collecting, processing, and using information to achieve the objective.
- Interpersonal role: Interacting with superiors, subordinates, outside stakeholders, and other.
- Decisional role: Selecting from alternative approaches and resolving conflicts, dilemmas, or challenges.

2. Characteristics of Management

- A well-known approaches to management:
  - POLC: Popular management theory using principles of management into planning, organizing, leading, and controlling



Planning & Organization

- **Planning**: process that develops, creates, and implements strategies for the accomplishment of objectives.
- Three levels of planning:
  1. **Strategic**: occurs at the highest levels of the organization (five or more years)
  2. **Tactical**: planning focuses on production planning and integrates organizational resources at a level below the entire enterprise (one to five years).
  3. **Operational**: focuses on the day-to-day operation of local resources
- **Organization**: structuring of resources to support the accomplishment of objectives.

Leadership & Controlling

- **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
- **Controlling**:
  - Monitoring progress toward completion
  - Making necessary adjustments to achieve the desired objectives
- Controlling function determines what must be monitored as well as using specific control tools to gather and evaluate information

3. Principles Of Information Security Management

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

InfoSec Planning

- **Planning** as part of InfoSec management
  - is an extension of the basic planning model discussed earlier.

- Included in the InfoSec planning model are
  - activities necessary to support the design, creation, and implementation of information security strategies as they exist within the IT planning environment

InfoSec Planning Types

- Several types of InfoSec plans exist:
  - Incident response
  - Business continuity
  - Disaster recovery
  - Policy
  - Personnel
  - Technology rollout
  - Risk management and
  - Security program including education, training and awareness

Policy

- **Policy**: set of organizational guidelines that dictates certain behavior within the organization

- In InfoSec, there are three general categories of policy:
  - General program policy (Enterprise Security Policy)
  - An issue-specific security policy (ISSP)
    - E.g., email, Intenert use
  - System-specific policies (SSSPs)
    - E.g., Access control list (ACLs) for a device

Programs

- **Programs** are operations managed as
  - specific entities in the information security domain
  - Example:
    - Security Education Training and Awareness (SETA) program.
  - Other programs that may emerge include
    - physical security program, complete with fire, physical access, gates, guards, and so on.

Protection

- Risk management activities, including
  - risk assessment and controls, and
- **Protection** mechanisms, technologies & tools
  - Each of these mechanisms represents some aspect of the management of specific controls in the overall security plan

People

- **People** are the most critical link in the information security program
- It is imperative that managers continuously recognize the crucial role that people play; includes
  - information security personnel and the security of personnel, as well as aspects of the SETA program

Project Management

- **Project management** discipline should be present throughout all elements of the information security program

- Involves
  - Identifying and controlling the resources applied to the project
  - Measuring progress and adjusting the process as progress is made toward the goal

2. Security Planning

Outline

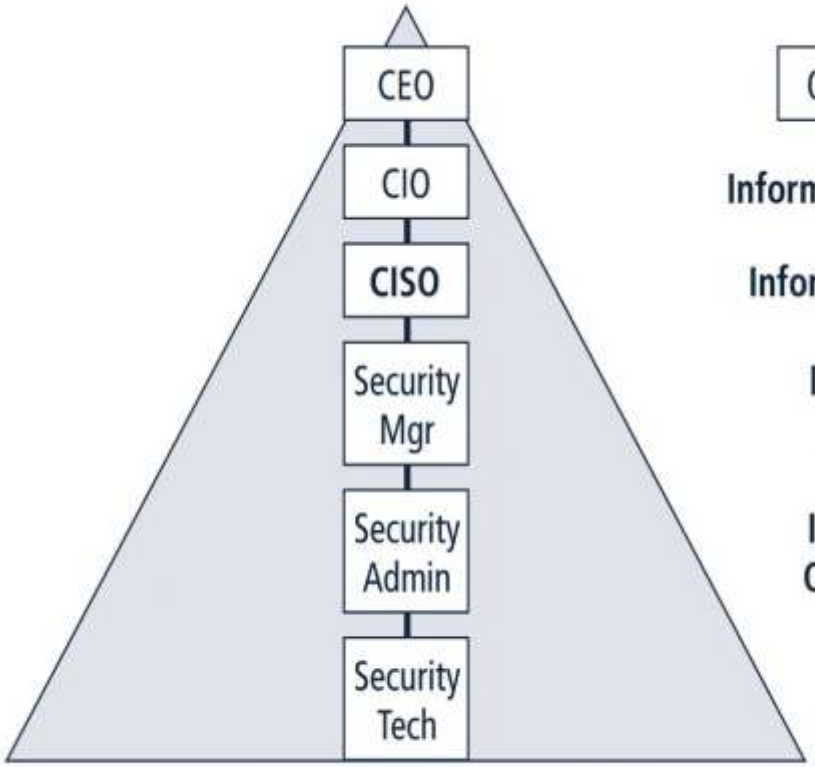
1. Introduction
2. Organizational Planning
3. The Security SDLC

1. Introduction

- **Planning:**
  - Is creating action steps toward goals, and then controlling them

- Planning process
  1. Organizational planning (in general and specific to information security)
  2. Preparedness planning, also called **contingency planning**.

2. Organizational Planning



1. Strategic
2. Tactical
3. Operational

Strategic Planning

- Strategy is the basis for long-term direction

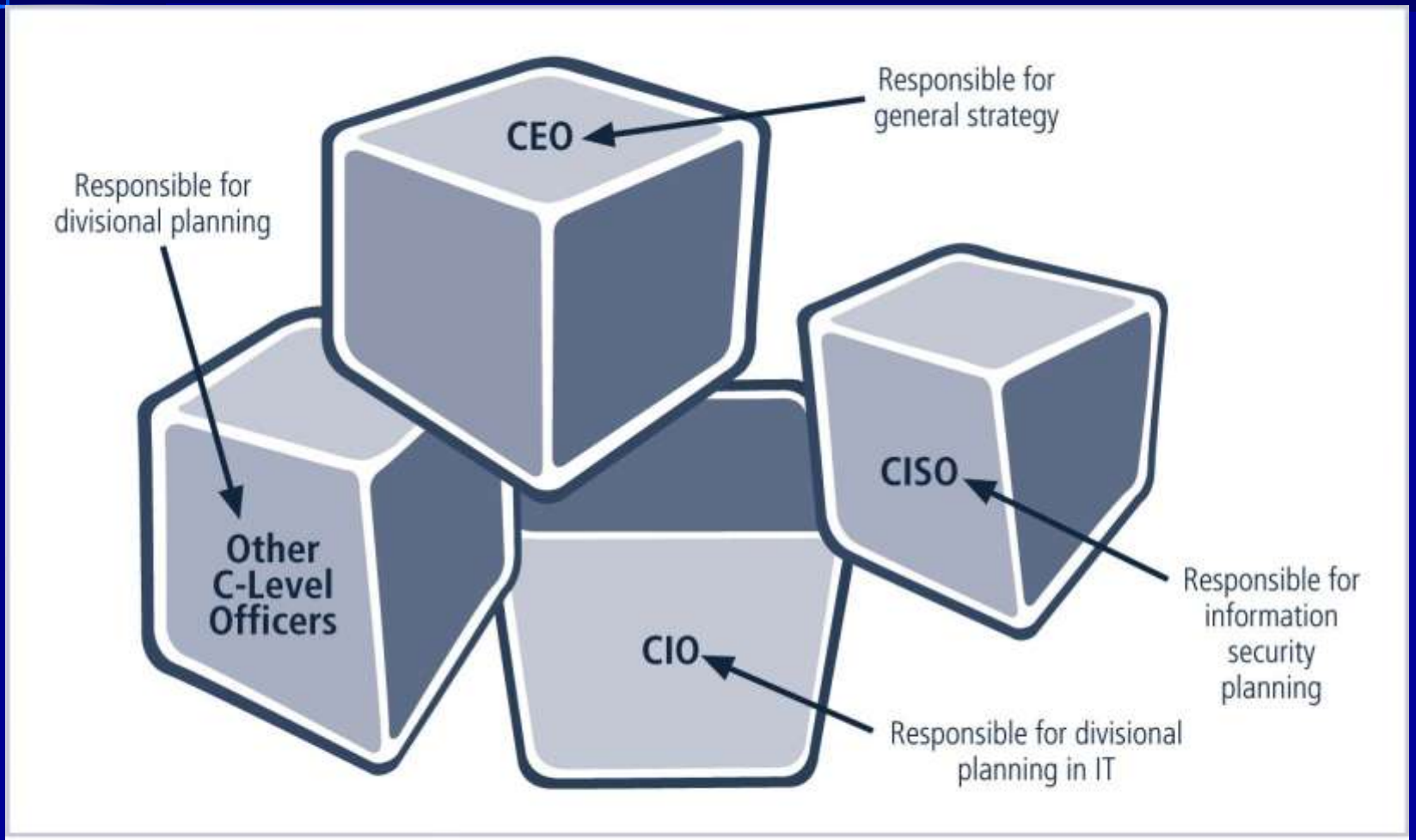
- Strategic planning:
  - Guides organizational efforts
  - Focuses resources on clearly defined goals

"… strategic planning is a disciplined effort to produce fundamental decisions and actions that shape and guide what an organization is, what it does, and why it does it, with a focus on the future."

Strategic Planning

- Organization:
  - Develops a general strategy
  - Creates specific strategic plans for major divisions
- Each level of division
  - translates those objectives into more specific objectives for the level below
- In order to execute this broad strategy,
  - executives must define individual managerial responsibilities

Strategic Planning



Tactical Planning

- Tactical Planning
  - Shorter focus than strategic planning
  - Usually one to three years
  - Breaks applicable strategic goals into a series of incremental objectives

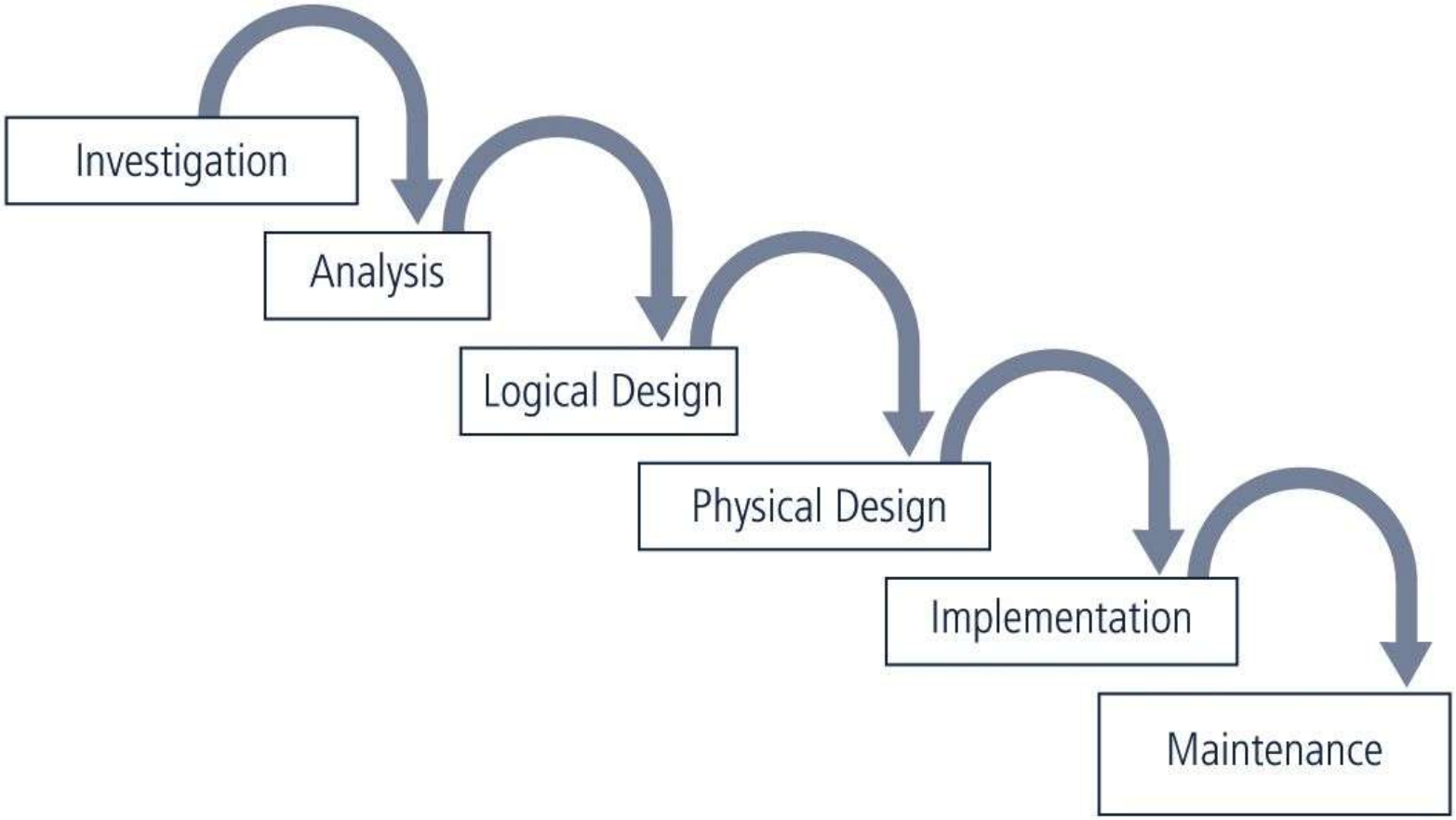
Operational Planning

- Operational Planning
  - Used by managers and employees to organize the ongoing, day-to-day performance of tasks
  - Includes clearly identified coordination activities across department boundaries such as:
    - Communications requirements
    - Weekly meetings
    - Summaries
    - Progress reports

3. The Security SDLC

- In general, the Security SDLC is similar to the SDCL
  - A methodology for the design and implementation of an information system in an organization.
- SecSDLC process involves:
  - Identification of specific threats and the risks that they represent
  - Subsequent design and implementation of specific controls to counter those threats and assist in the management of the risk those threats pose to the organization

SecSDLC


Investigation
Analysis
Logical Design
Physical Design
Implementation
Maintenance

Investigation in the SecSDLC

- **Investigation** often begins as directive from management specifying the process, outcomes, and goals of the project and its budget
- Frequently begins with the affirmation or creation of security policies
- Teams assembled to analyze problems, define scope, specify goals and identify constraints
- Feasibility analysis determines whether the organization has resources and commitment to conduct a successful security analysis and design

Analysis in the SecSDLC

- A preliminary **analysis** of existing security policies or programs is prepared along with known threats and current controls
- Includes an analysis of relevant legal issues that could affect the design of the security solution
- **Risk management** begins in this stage

Risk Management

- **Risk Management**: process of identifying, assessing, and evaluating the levels of risk facing the organization
  - Specifically the threats to the information stored and processed by the organization
- To better understand the analysis phase of the SecSDLC, you should know something about the kinds of threats facing organizations
- In this context, a threat is an object, person, or other entity that represents a constant danger to an asset

Risk Management

- Use some method of prioritizing risk posed by each category of threat and its related methods of attack
- To manage risk, you must identify and assess the value of your information assets
- Risk assessment assigns comparative risk rating or score to each specific information asset

  Risk management identifies vulnerabilities in an organization's information systems and takes carefully reasoned steps to assure the confidentiality, integrity, and availability of all the components in organization's information system

Design in the SecSDLC

- Design phase actually consists of two distinct phases:
  - Logical design phase: team members create and develop a blueprint for security, and examine and implement key policies
  - Physical design phase: team members evaluate the technology needed to support the security blueprint, generate alternative solutions, and agree upon a final design
- Between the logical and physical design phases, a security manager may seek to use established **security models** to guide the design process.

Security Models

- Security managers often use established security models to guide the design process
- Security models provide frameworks for ensuring that all areas of security are addressed
- Organizations can adapt or adopt a framework to meet their own information security needs

Policy

- A critical design element of the information security program is the information security policy
- Management must define three types of security policy:
  - General or security program policy (GSP)
  - Issue-specific security policies (ISSP)
  - Systems-specific security policies (SSSP)

SETA

- An integral part of the InfoSec program is
  - Security education and training (SETA) program
  - SETA program consists of three elements:
    - security education, security training, and security awareness
- Purpose of SETA is to enhance security by:
  - Improving awareness
  - Developing skills and knowledge
  - Building in-depth knowledge

Design

- Attention turns to the design of the controls and safeguards used to protect information from attacks by threats

- Three categories of controls:
  - Managerial
  - Operational
  - Technical

Managerial Controls

- Address design/implementation of the
  - security planning process and
  - security program management

- Management controls also address:
  - Risk management
  - Security control reviews

  - Legal compliance and maintenance of the entire security life cycle

Operational Controls

- Cover management functions and lower level planning including:
  - Disaster recovery
  - Incident response planning
- Operational controls also address:
  - Personnel security
  - Physical security
  - Protection of production inputs and outputs

Technical Controls

- Address those tactical and technical issues related to
  - designing and implementing security in the organization
- Technologies necessary to protect information are examined and selected

Contingency Planning

- Essential preparedness documents provide contingency planning (CP) to prepare, react and recover from circumstances that threaten the organization:
  - Incident response planning (IRP)
  - Disaster recovery planning (DRP)
  - Business continuity planning (BCP)

Implementation in the SecSDLC

- Security solutions are acquired, tested, implemented, and tested again
- Personnel issues are evaluated and specific training and education programs conducted
- Perhaps most important element of implementation phase is management of project plan:
  - Planning the project
  - Supervising tasks and action steps within the project
  - Wrapping up the project

InfoSec Project Team

- Should consist of individuals experienced in one or multiple technical and non-technical areas including:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

InfoSec Professionals

- It takes a wide range of professionals to support a diverse information security program:
  - Chief Information Officer (CIO)
  - Chief Information Security Officer (CISO)
  - Security Managers
  - Security Technicians
  - Data Owners
  - Data Custodians
  - Data Users

Maintenance in the SecSDLC

- Once information security program is implemented,
  - it must be properly operated, managed, and kept up to date by means of established procedures
- If the program is not adjusting adequately to the changes in the internal or external environment, it may be necessary to begin the cycle again

3. Contingency Planning

Outline

1. Introduction
2. Incident Response
3. Disaster Recovery
4. Business Continuity

Introduction

- Planning for the unexpected event
  - the use of technology is interrupted
- Procedures are required in order to stand up to unexpected events
- The overall planning for unexpected events is called contingency planning (CP).

What Is Contingency Planning?

- It is how organizational planners position their organizations to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets.
- Main goal: restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event.

CP Components

- Incident response planning (IRP) focuses on immediate response
- Disaster recovery planning (DRP) focuses on restoring operations at the primary site after disasters occur
- Business continuity planning (BCP) facilitates establishment of operations at an alternate site

CP Components (Continued)

- To ensure continuity across all CP processes during planning process, contingency planners should:
  - Identify the mission- or business-critical functions
  - Identify resources that support critical functions
  - Anticipate potential contingencies or disasters
  - Select contingency planning strategies
  - Implement selected strategy
  - Test and revise contingency plans

Incident Response Plan

- IRP:
  - Detailed set of processes and procedures that anticipate, detect, and mitigate the impact of an unexpected event that might compromise information resources and assets

- Incident response (IR):
  - Set of procedures that commence when an incident is detected

Incident Response Plan (Continued)

- When a threat becomes a valid attack, it is classified as an **information security incident** if:
  - It is directed against information assets
  - It has a realistic chance of success
  - It threatens the confidentiality, integrity, or availability of information assets

- It is important to understand that IR is a reactive measure, not a preventive one

Disaster Recovery

- Preparation for and recovery from a disaster
  - whether natural or man made
- In general, an incident is a **disaster** when:
  - organization is unable to contain or control the impact of an incident, or
  - level of damage or destruction from incident is so severe, the organization is unable to quickly recover
- Key role of DRP: defining how to reestablish operations at location where organization is usually located