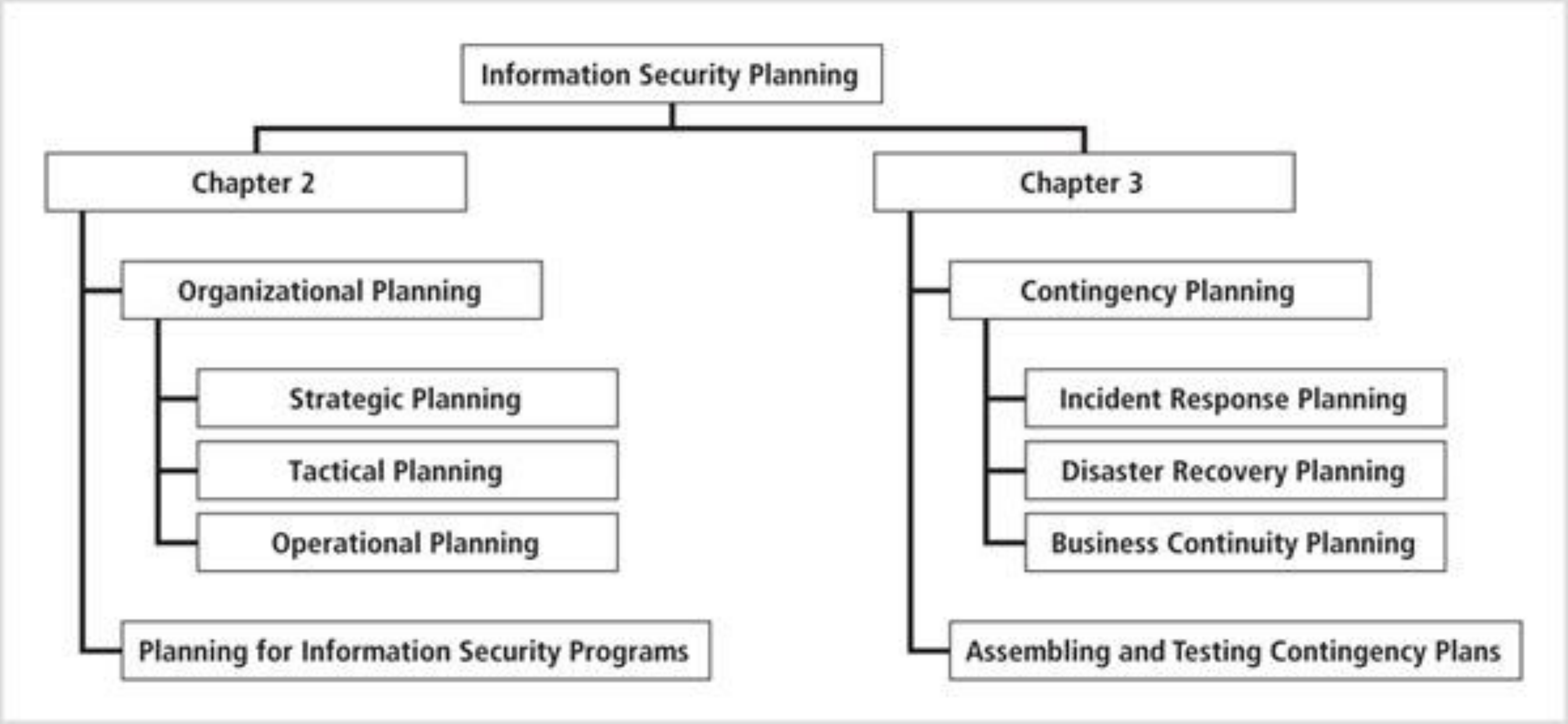
CSIT988/CSIT488
Security, Ethics and Professionalism
Week 4: Planning for Contingencies

Subject Coordinator: *Dr Khoa Nguyen*

School of Computing and Information Technology

Autumn 2025

Information Security Planning



Information Security Planning

Chapter 2

Organizational Planning

Strategic Planning

Tactical Planning

Operational Planning

Planning for Information Security Programs

Chapter 3

Contingency Planning

Incident Response Planning

Disaster Recovery Planning

Business Continuity Planning

Assembling and Testing Contingency Plans

Why Contingency Planning?

- **Goal:** planning for unexpected adverse events, when the use of technology is disrupted and business operations come close to a standstill.

- Planning for an unexpected adverse event usually involves managers from among general business management as well as the information technology (IT) and the InfoSec communities of interest.

- The need to have a plan in place that systematically addresses how to identify, contain, and resolve an unexpected adverse event was identified in the earliest days of IT.

Why Contingency Planning?

- As advised by NIST:

  “Because information system resources are essential to an organization’s success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption.”

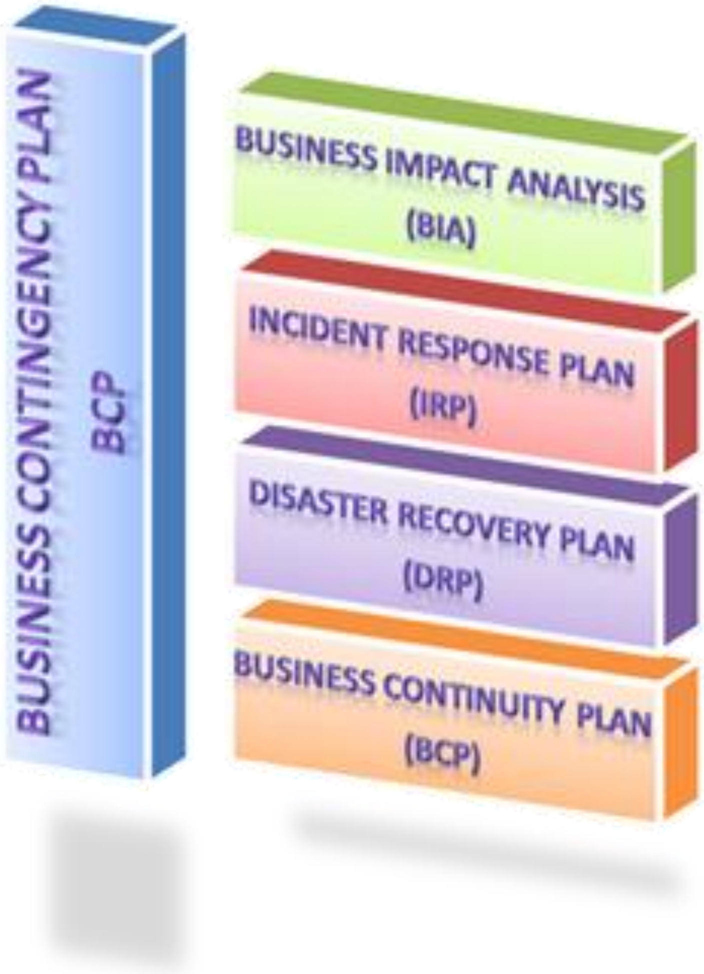
- The Hartford insurance company estimates that:

  On average, over 40 percent of businesses that don’t have a disaster plan go out of business after a major loss like a fire, a break-in, or a storm.

Fundamentals of Contingency Planning

- **Contingency planning (CP)**
  - The overall planning for unexpected events
  - Involves preparing for, detecting, reacting to, and recovering from events that threaten the security of information resources and assets
- **Main goal**
  - The restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event

Components of Contingency Planning

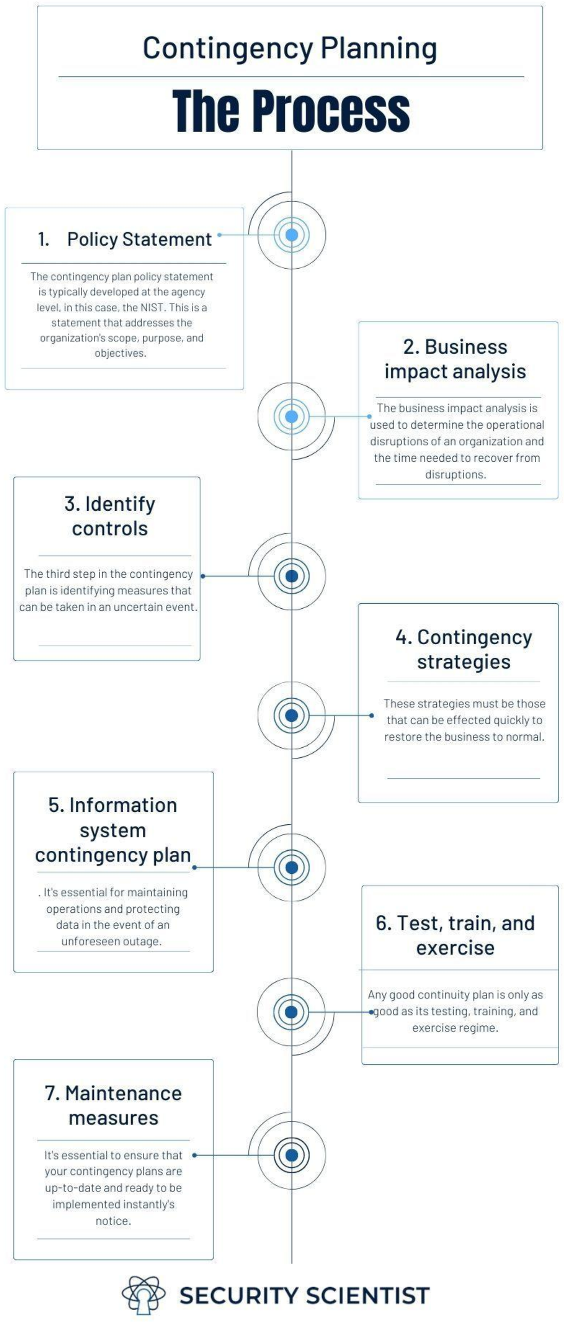


- **Business impact analysis (BIA):** A preparatory activity common to both CP and Risk Management; determines which functions and information systems are the most critical to the success of the organization
- **Incident response planning (IRP):** Focuses on immediate response
- **Disaster recovery planning (DRP):** Focuses on restoring operations at the primary site after disasters occur
- **Business continuity planning (BCP):** Facilitates establishment of operations at an alternate site, until the organization is able to resume operations at its primary site or select a new primary location

- Ideally, the CIO, the CISO, and key IT and business managers should be actively involved during the creation and development of all CP components

- Once formed, the contingency planning management team (CPMT) begins developing a CP document, for which NIST recommends using the following 7 steps:

  1. Develop the CP policy statement
  2. Conduct the BIA
  3. Identify preventive controls
  4. Create contingency strategies
  5. Develop a contingency plan
  6. Ensure plan testing, training, and exercises
  7. Ensure plan maintenance



Contingency Planning

The Process

1. Policy Statement

The contingency plan policy statement is typically developed at the agency level, in this case, the NIST. This is a statement that addresses the organization's scope, purpose, and objectives.

2. Business impact analysis

The business impact analysis is used to determine the operational disruptions of an organization and the time needed to recover from disruptions.

3. Identify controls

The third step in the contingency plan is identifying measures that can be taken in an uncertain event.

4. Contingency strategies

These strategies must be those that can be effected quickly to restore the business to normal.

5. Information system contingency plan

. It's essential for maintaining operations and protecting data in the event of an unforeseen outage.

6. Test, train, and exercise

Any good continuity plan is only as good as its testing, training, and exercise regime.

7. Maintenance measures

It's essential to ensure that your contingency plans are up-to-date and ready to be implemented instantly's notice.

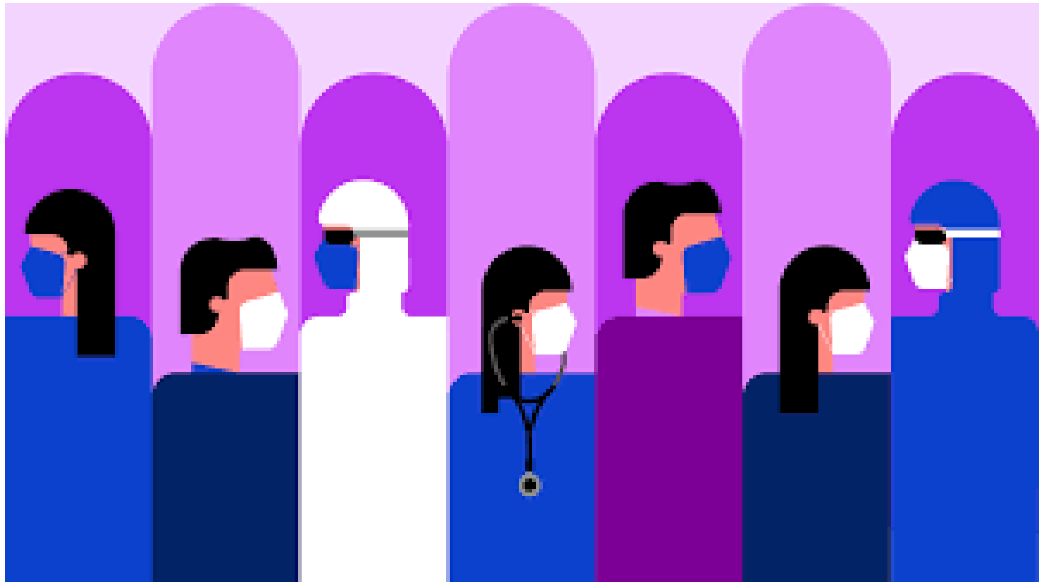
SECURITY SCIENTIST

Developing CP Document Process

1. Develop the contingency planning policy statement: Provides the authority and guidance necessary to develop an effective contingency plan
2. Conduct the BIA: Helps to identify and prioritize critical IT systems and components
3. Develop recovery strategies: Ensure that the system may be recovered quickly and effectively following a disruption
4. Identify preventive controls: Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs
5. Develop an IT contingency plan: Contains detailed guidance and procedures for restoring a damaged system
6. Ensure plan testing, training, and exercises: Testing the plan identifies planning gaps; Training prepares recovery personnel for plan activation; Both activities improve plan effectiveness and overall agency preparedness
7. Ensure plan maintenance: The plan should be updated regularly to remain current with system enhancements

Four teams are involved in contingency planning and contingency operations

- The CP management team (CPMT)
- The incident response (IR) team
- The disaster recovery (DR) team
- The business continuity plan (BC) team



CPMT

- Collects information about information systems and about the threats they face, conducts the business impact analysis, then creates the contingency plans for incident response, disasters response and business continuity.

- The CP team should include
  - ➢ Champion
  - ➢ Project Manager
  - ➢ Team Members
    - ✓ Business managers
    - ✓ Information technology managers
    - ✓ Information security managers

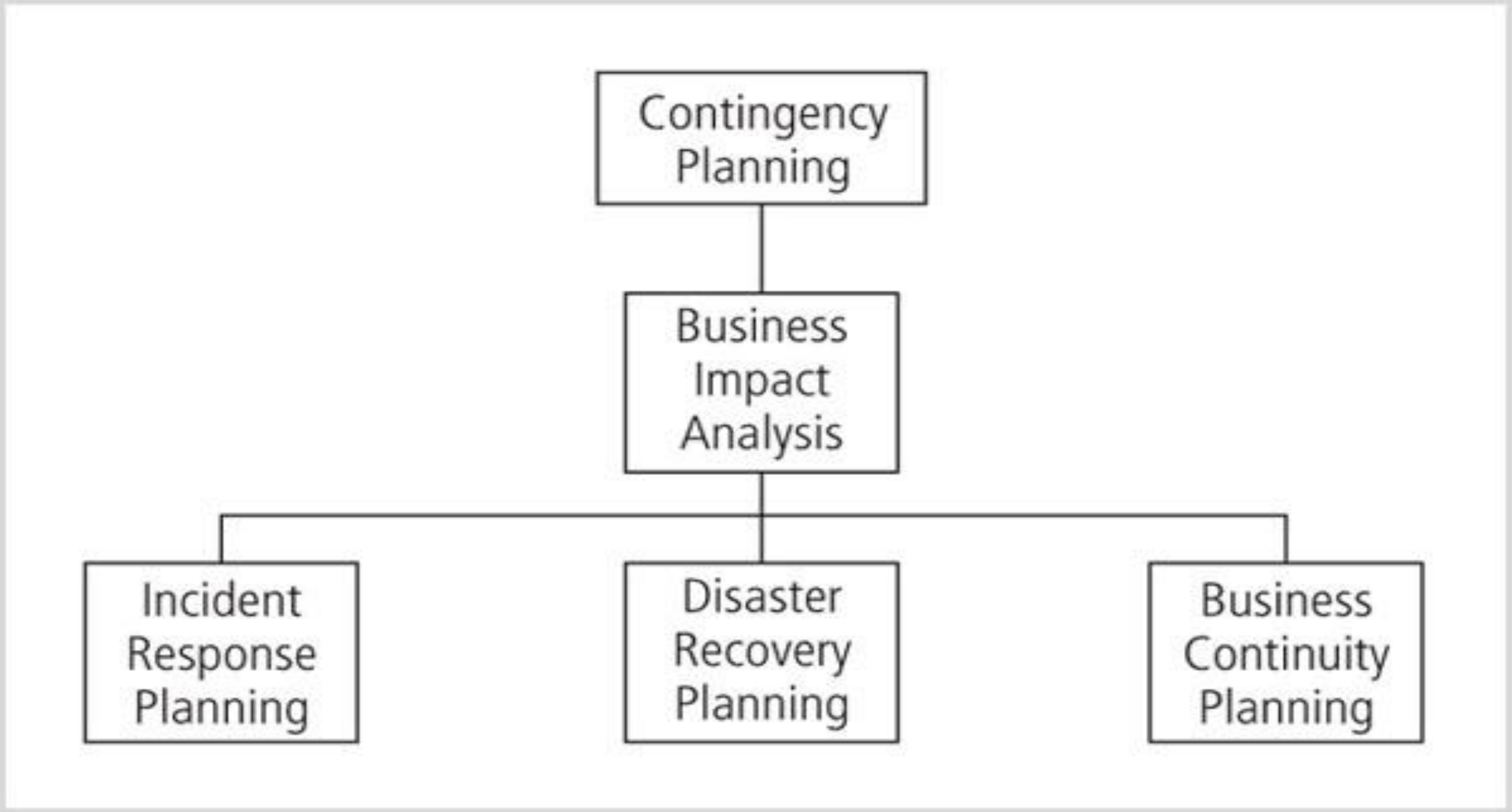
IR, DR and BC Teams

- **Incident response team**: manages and executes the IR plan by detecting, evaluating and responding to incidents.

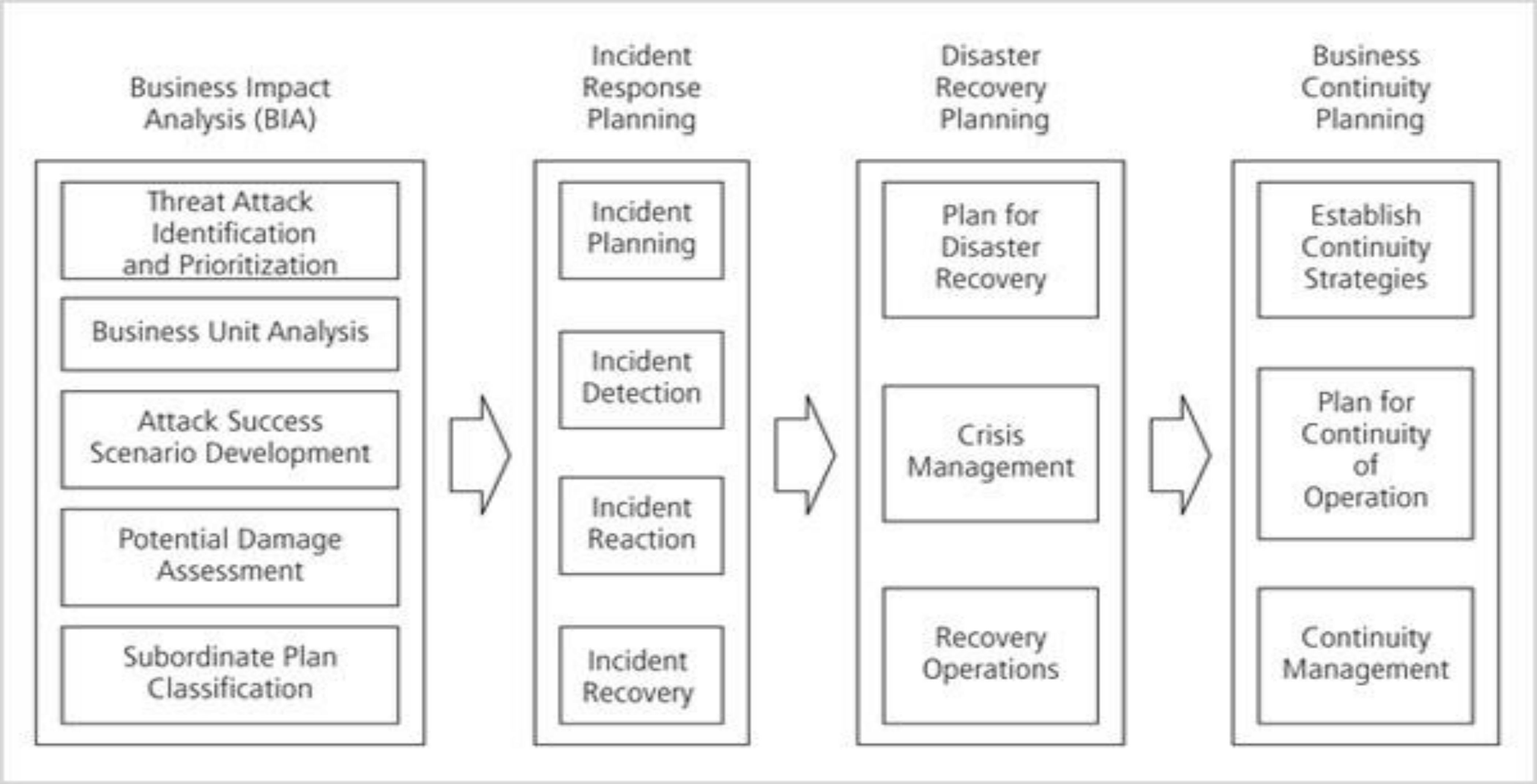
- **Disaster recovery team**: manages and executes the DR plan by detecting, evaluating and responding to disasters and by re-establishing operations at the primary business site

- **Business continuity team**: manages and executes the BC plan by setting up and starting off-site operations in the event of an incident or disaster.

Components of Contingency Planning


Contingency Planning
Business Impact Analysis
Incident Response Planning
Disaster Recovery Planning
Business Continuity Planning

Major Tasks in CP



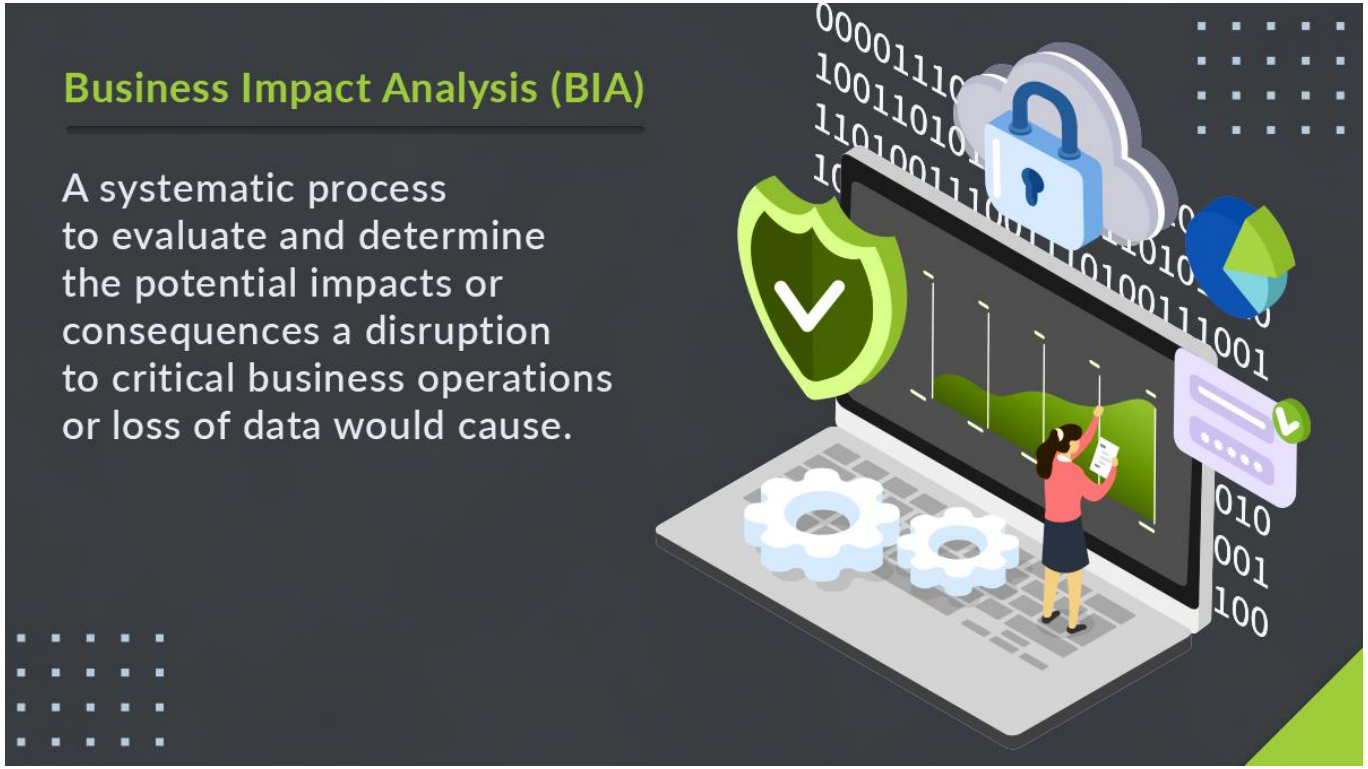
Business Impact Analysis (BIA)
- Threat Attack Identification and Prioritization
- Business Unit Analysis
- Attack Success Scenario Development
- Potential Damage Assessment
- Subordinate Plan Classification

Incident Response Planning
- Incident Planning
- Incident Detection
- Incident Reaction
- Incident Recovery

Disaster Recovery Planning
- Plan for Disaster Recovery
- Crisis Management
- Recovery Operations

Business Continuity Planning
- Establish Continuity Strategies
- Plan for Continuity of Operation
- Continuity Management

- Provides the CP team with information about systems and the threats they face
  - ➢ First phase in the CP process
  - ➢ A crucial component of the initial planning stages
  - ➢ Provides detailed scenarios of each potential attack’s impact



Business Impact Analysis (BIA)

A systematic process to evaluate and determine the potential impacts or consequences a disruption to critical business operations or loss of data would cause.

Business Impact Analysis (BIA)

- BIA is not Risk Management (which focuses on identifying threats, vulnerabilities, and attacks to determine controls)
- BIA assumes controls have been bypassed or are ineffective, and attack was successful
  - ➢ By assuming the worst has happened, then assessing how that adversity will impact the organization, insight is gained regarding how the organization must respond to the adverse event, minimize the damage, recover from the effects, and return to normal operations.

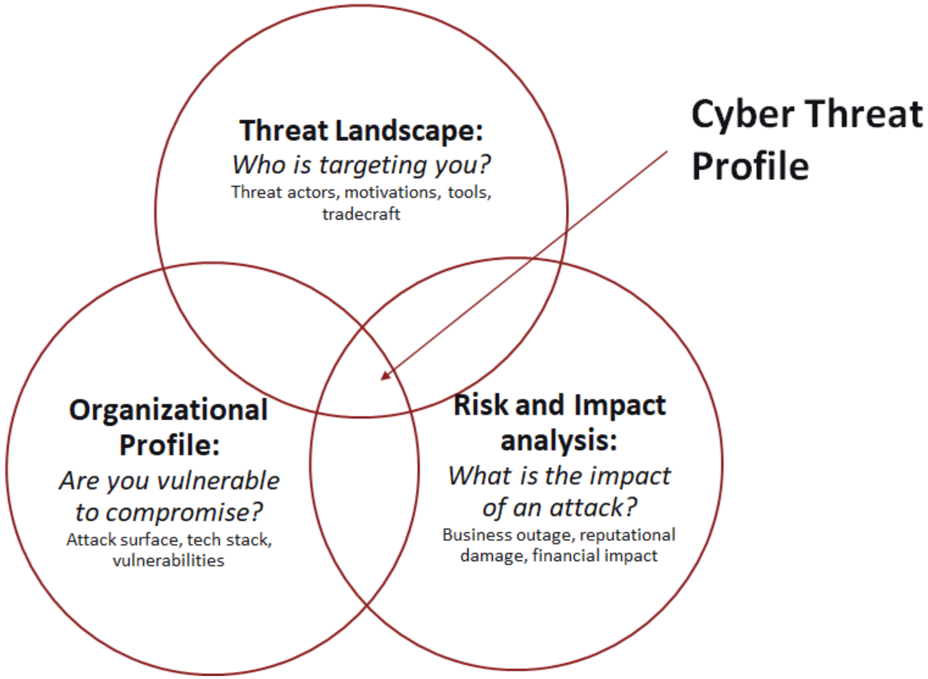
Business Impact Analysis (cont'd.)

The CP team conducts the BIA in the following stages:

- Threat attack identification
- Business unit analysis
- Attack success scenario development
- Potential damage assessment
- Subordinate plan classification

BIA Stages

- **Threat attack identification:** An organization that uses a risk management process will have identified and prioritized threats
  - Update threat list and add one additional piece of information - the attack profile (a detailed description of activities that occur during an attack)
- **Business unit analysis:** the analysis and prioritization of business functions within the organization


Threat Landscape:
Who is targeting you?
Threat actors, motivations, tools, tradecraft
Organizational Profile:
Are you vulnerable to compromise?
Attack surface, tech stack, vulnerabilities
Risk and Impact analysis:
What is the impact of an attack?
Business outage, reputational damage, financial impact
Cyber Threat Profile

BIA Stages

- **Attack success scenario development:** creating a series of scenarios depicting impact of successful attack on each functional area
- Attack profiles should include scenarios depicting typical attack including:
  - Methodology
  - Indicators
  - Broad consequences
- Add alternate outcomes
  - Best case, worst case, and most likely

BIA Stages

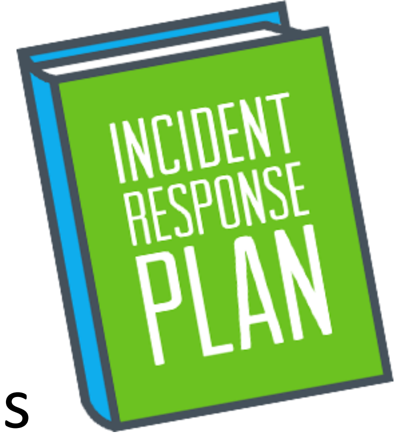
- **Potential damage assessment:** Estimating the cost of the best, worst, and most likely outcomes
  - By preparing an attack scenario end case
  - Allows identification of what must be done to recover from each possible case

- **Subordinate plan classification:** Each attack scenario end case is categorized as disastrous or not
  - Disastrous attacks require disaster recovery plan
  - Non-disastrous attacks require incident response plan

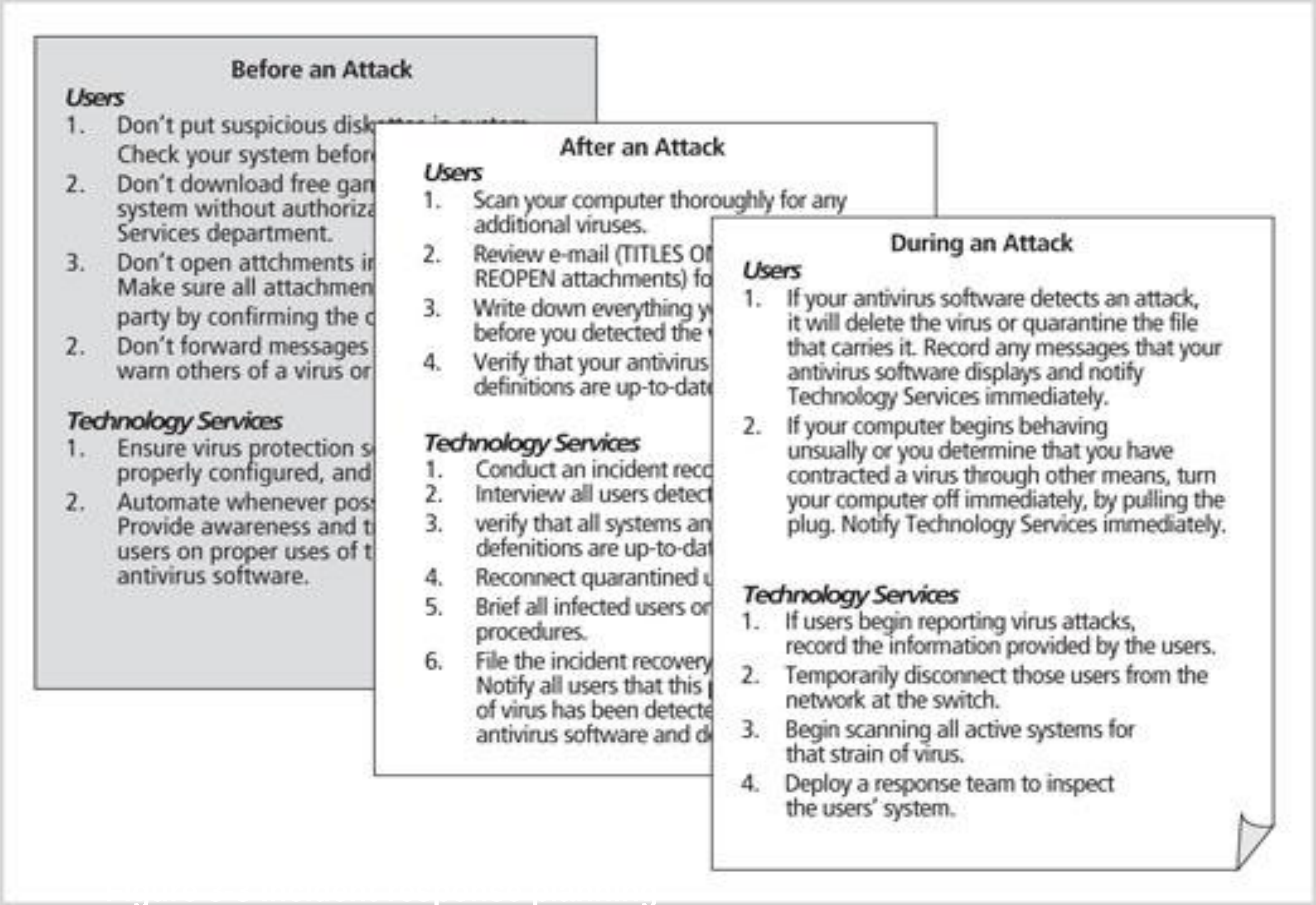
Incident Response Plan vs Disaster Recovery Plan

Incident response and disaster recovery plans are two similar yet different components of a strong cyber security system.

Incident Response Plan



- **Incident response plan:** A detailed set of processes and procedures that anticipate, detect, and mitigate the impact of an unexpected event that might compromise information resources and assets
  - ➢ Procedures commence when an incident is detected
- When a threat becomes a valid attack, it is classified as an InfoSec incident if: It is directed against information assets; It has a realistic chance of success; It threatens the CIA of information assets
- Incident response is a reactive measure, not a preventative one
- An early task for the CPMT is to form a **computer security incident response team** (CSIRT). Key members of the CSIRT become the IR planning committee.



Before an Attack

Users

1. Don't put suspicious disk
   Check your system befor
2. Don't download free gam
   system without authoriz
   Services department.
3. Don't open attchments i
   Make sure all attachmen
   party by confirming the
2. Don't forward messages
   warn others of a virus or

Technology Services

1. Ensure virus protection s
   properly configured, and
2. Automate whenever pos
   Provide awareness and t
   users on proper uses of t
   antivirus software.

After an Attack

Users

1. Scan your computer thoroughly for any additional viruses.
2. Review e-mail (TITLES O
   REOPEN attachments) fo
3. Write down everything y
   before you detected the
4. Verify that your antivirus
   definitions are up-to-dat

Technology Services

1. Conduct an incident reco
2. Interview all users detect
3. verify that all systems an
   defenitions are up-to-dat
4. Reconnect quarantined
5. Brief all infected users o
   procedures.
6. File the incident recovery
   Notify all users that this
   of virus has been detecte
   antivirus software and d

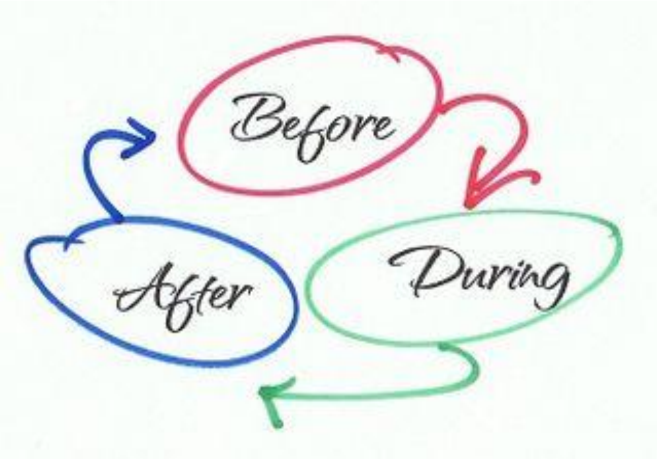
During an Attack

Users

1. If your antivirus software detects an attack, it will delete the virus or quarantine the file that carries it. Record any messages that your antivirus software displays and notify Technology Services immediately.
2. If your computer begins behaving unsually or you determine that you have contracted a virus through other means, turn your computer off immediately, by pulling the plug. Notify Technology Services immediately.

Technology Services

1. If users begin reporting virus attacks, record the information provided by the users.
2. Temporarily disconnect those users from the network at the switch.
3. Begin scanning all active systems for that strain of virus.
4. Deploy a response team to inspect the users' system.



- **During the incident:** Planners develop and document the procedures that must be performed during the incident
  - ➢ These procedures are grouped and assigned to various roles
  - ➢ The IR planning committee drafts a set of function-specific procedures

- **After the incident:** Planners develop and document the procedures that must be performed immediately after the incident has ceased.

- **Before at the incident:** Develop procedures for tasks that must be performed in advance of the incident: Details of data backup schedules; Disaster recovery preparation; Training schedules; Testing plans; Copies of service agreements; Business continuity plans

Incident Response Plan (cont'd.)

- IR planning requires a detailed understanding of the information systems and the threats they face. The IR planning team seeks to develop pre-defined responses that guide users through the steps needed to respond to an incident
  - Enables rapid reaction without confusion or wasted time and effort

- **CSIRT:** a subset of the IR team, composed of technical and managerial IT and InfoSec professionals prepared to diagnose and respond to an incident.
- Each member of the IR team must know his or her specific role, work in concert with each other, and execute the objectives of the IRP

Incident Response Plan (cont’d.)

- **Incident classification**
  - Determine whether an event is an actual incident
  - May be challenging
  - Uses initial reports from end users, intrusion detection systems, host- and network-based virus detection software, and systems administrators
  - Careful training allows everyone to relay vital information to the IR team

- Three categories of incident indicators: possible, probable and definite (according to Donald L. Pipkin).

Incident Indicators

- **Possible indicators:** Presence of unfamiliar files; Presence or execution of unknown programs or processes; Unusual consumption of computing resources; Unusual system crashes

- **Probable indicators:** Activities at unexpected times; Presence of new accounts; Reported attacks; Notification from IDS

- **Definite indicators:** Use of dormant accounts; Changes to logs; Presence of hacker tools; Notifications by partner or peer; Notification by hacker

Incident Response Plan (cont’d.)

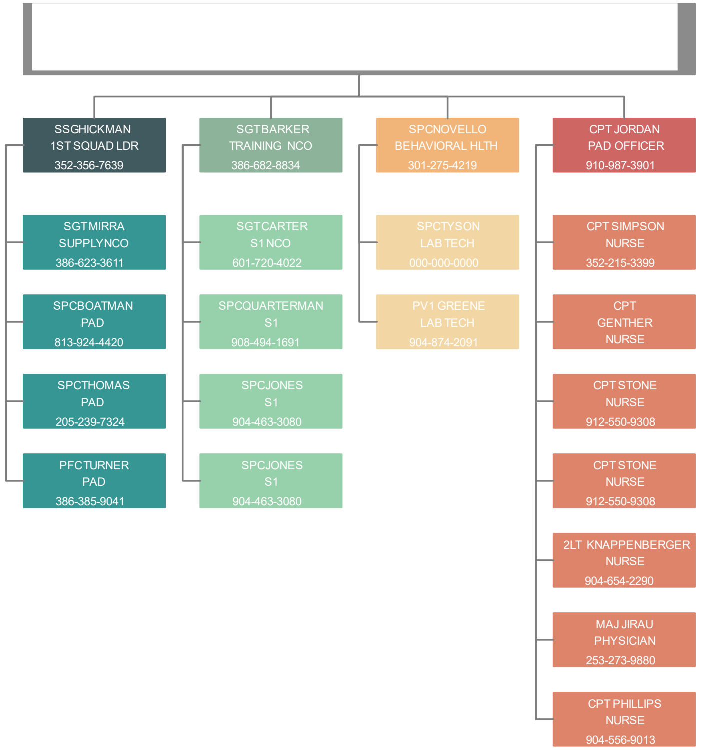
- When the following actual incidents are confirmed, the corresponding IR must be immediately activated:
  - ➢ Loss of availability
  - ➢ Loss of integrity
  - ➢ Loss of confidentiality
  - ➢ Violation of policy
  - ➢ Violation of law

- The IR team moves from the detection phase to the reaction phase
  - ➢ Action steps taken by the CSIRT must occur quickly/concurrently: notification of key personnel, the assignment of tasks, and documentation of the incident

Incident Response Plan (cont'd.)

Alert roster

- A document containing contact information on the individuals to be notified in the event of an actual incident either sequentially or hierarchically
- The alert message is a scripted description of the incident
- Other key personnel must be notified of the incident after the incident has been confirmed, but before media or other external sources learn of it



SSGHICKMAN
1ST SQUAD LDR
352-356-7639

SGTMIRRA
SUPPLYNCO
386-623-3611

SPCBOATMAN
PAD
813-924-4420

SPCTHOMAS
PAD
205-239-7324

PFCTURNER
PAD
386-385-9041

SGTBARKER
TRAINING NCO
386-682-8834

SGTCARTER
S1 NCO
601-720-4022

SPCQUARTERMAN
S1
908-494-1691

SPCJONES
S1
904-463-3080

SPCJONES
S1
904-463-3080

SPCNOVELLO
BEHAVIORAL HLTH
301-275-4219

SPCTYSON
LAB TECH
000-000-0000

PV1 GREENE
LAB TECH
904-874-2091

CPT JORDAN
PAD OFFICER
910-987-3901

CPT SIMPSON
NURSE
352-215-3399

CPT
GENTHER
NURSE

CPT STONE
NURSE
912-550-9308

CPT STONE
NURSE
912-550-9308

2LT KNAPPENBERGER
NURSE
904-654-2290

MAJ JIRAU
PHYSICIAN
253-273-9880

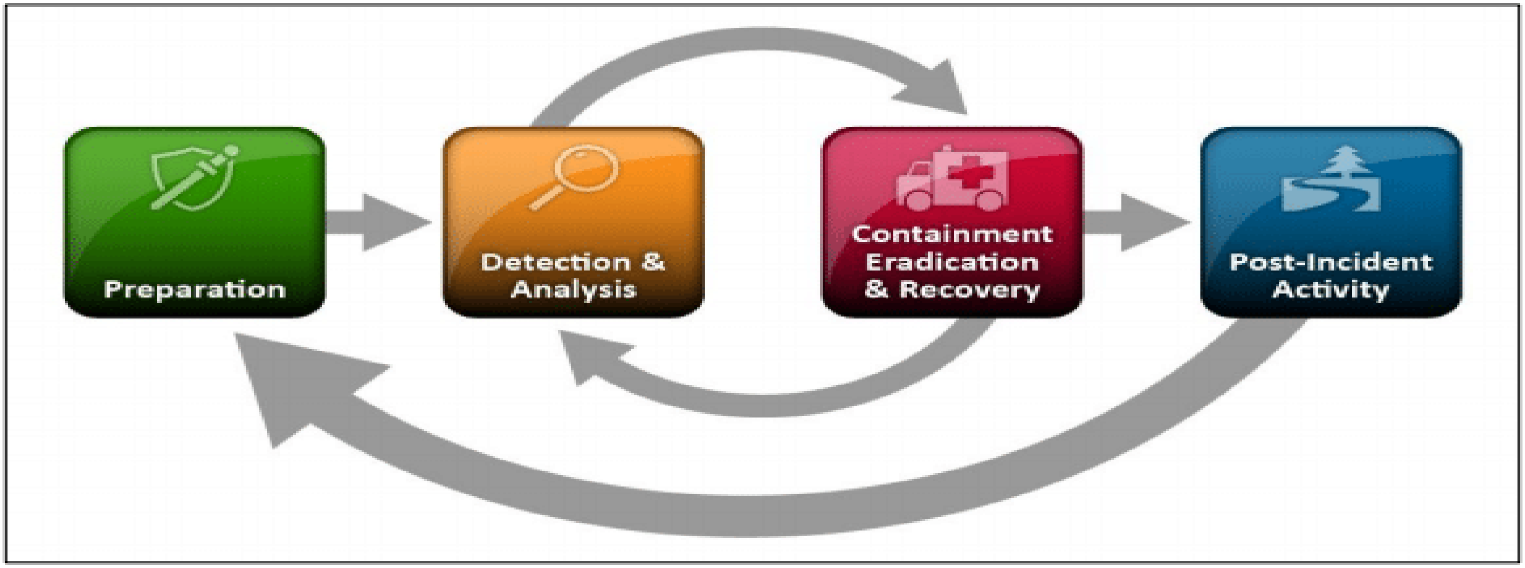
CPT PHILLIPS
NURSE
904-556-9013

Incident Response Plan (cont’d.)

Documentation

- Begins once an incident has been confirmed and the notification process is underway
- Record the who, what, when, where, why and how of each action taken during the incident
- Serves as a case study after the fact to determine if the right actions were taken, and if they were effective
- Can also prove the organization did everything possible to deter the spread of the incident

Incident Response Plan (cont'd.)



- The essential task of IR is to stop the incident or contain its impact

- Incident containment strategies focus on two tasks
  - ➢Stopping the incident
  - ➢Recovering control of the systems

Incident Response Plan (cont’d.)

- **Containment strategies**
  - Disconnect the affected communication circuits
  - Dynamically apply filtering rules to limit certain types of network access
  - Disabling compromised user accounts
  - Reconfiguring firewalls to block the problem traffic
  - Temporarily disabling the compromised process or service
  - Taking down the conduit application or server (e.g. e-mail server)
  - Stopping all computers and network devices

Incident Response Plan (cont’d.)

- **Incident escalation:** An incident may increase in scope or severity to the point that the IRP cannot adequately contain the incident
  - ➢ Each organization will have to determine, during the business impact analysis, the point at which the incident becomes a disaster

- The organization must also document when to involve outside response

Incident Response Plan (cont’d.)

- **Recovering from Incidents:** Once contained and system control regained, incident recovery can begin
  - ➢ The CSIRT must assess the full extent of the damage in order to determine what must be done to restore the systems

- **Incident damage assessment:** Determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets
  - ➢ Those who document the damage must be trained to collect and preserve evidence, in case the incident is part of a crime or results in a civil action

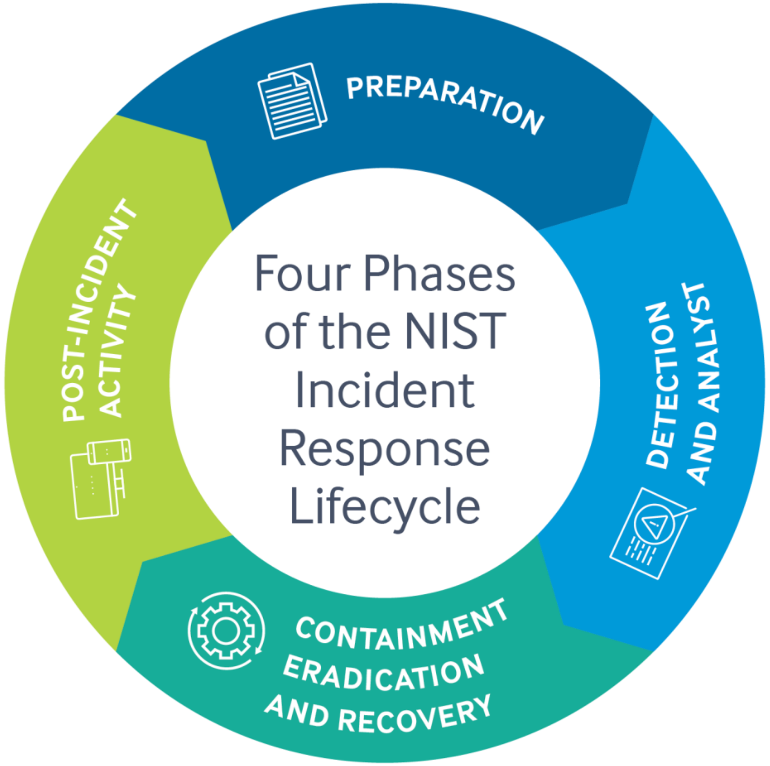
Incident Response Plan (cont'd.)

Recovery process (according to Donald L. Pipkin)

- Identify the vulnerabilities that allowing the incident to occur and spread and resolve them
- Address the safeguards that failed to stop or limit the incident, or were missing from the system in the first place and install, replace or upgrade them
- Evaluate monitoring capabilities (if present) to improve detection and reporting methods, or install new monitoring capabilities
- Restore the data from backups as needed
- Restore the services and processes in use where compromised (and interrupted) services and processes must be examined, cleaned, and then restored
- Continuously monitor the system
- Restore the confidence of the members of the communities of interest

Incident Response Plan (cont'd.)

- Before returning to routine duties, the CSIRT must conduct an after-action review (AAR)
  - ➢ A detailed examination of the events that occurred
  - ➢ All team members review their actions during the incident and identify areas where the IR plan worked, didn't work, or should improve
- When an incident violates civil/criminal law, notify the proper authorities. Involving law enforcement has both advantages and disadvantages
  - ➢ Better equipped at processing evidence, obtaining statements from witnesses, and building legal cases
  - ➢ Can result in loss of control of the chain of events following an incident



PREPARATION
DETECTION AND ANALYST
CONTAINMENT ERADICATION AND RECOVERY
POST-INCIDENT ACTIVITY
Four Phases of the NIST Incident Response Lifecycle

Disaster Recovery Plan

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

Disaster Recovery Plan (cont'd.)

A DRP can classify disasters in a number of ways

- ➢ The most common method is to separate natural disasters from man-made disasters

- ➢ Another way of classifying disasters is by speed of development
  - ✓ Rapid onset disasters
  - ✓ Slow onset disasters

Disaster Recovery Plan (cont’d.)

- Scenario development and impact analysis
  - ➢ Used to categorize the level of threat of each potential disaster

- DRP must be tested regularly

- Key points in the DRP
  - ➢ Clear delegation of roles and responsibilities
  - ➢ Execution of the alert roster and notification of key personnel
  - ➢ Clear establishment of priorities
  - ➢ Documentation of the disaster
  - ➢ Action steps to mitigate the impact
  - ➢ Alternative implementations for systems components

Disaster Recovery Plan (cont’d.)

- Actual events often outstrip even the best of plans
  - To be prepared, DRP should be flexible

- If physical facilities are intact, begin restoration
  - If organization’s facilities are unusable, take alternative actions
  - When disaster threatens the organization at the primary site, DRP becomes BCP

Business Continuity Plan

- Ensures critical business functions can continue in a disaster

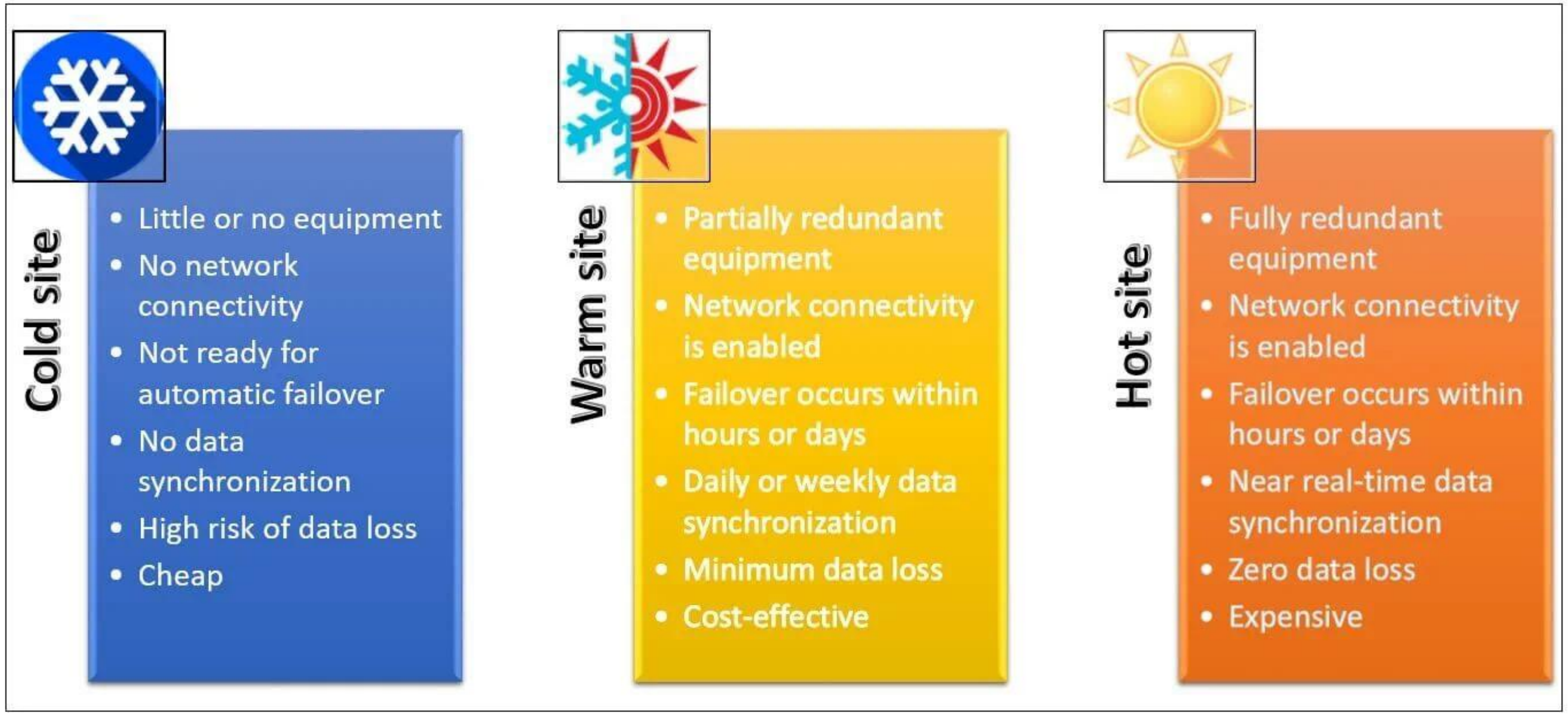
- Managed by CEO of the organization

- Activated and executed concurrently with the DRP when needed
  - While BCP reestablishes critical functions at alternate site, DRP focuses on reestablishment at the primary site

Business Continuity Plan (cont’d.)

- Relies on identification of critical business functions and the resources to support them
- **Continuity strategies**
  - ➢ Exclusive-use options: hot, warm and cold sites
  - ➢ Shared-use options: timeshare, service bureaus, mutual agreements

- Determining factor is usually cost



Cold site

- Little or no equipment
- No network connectivity
- Not ready for automatic failover
- No data synchronization
- High risk of data loss
- Cheap

Warm site

- Partially redundant equipment
- Network connectivity is enabled
- Failover occurs within hours or days
- Daily or weekly data synchronization
- Minimum data loss
- Cost-effective

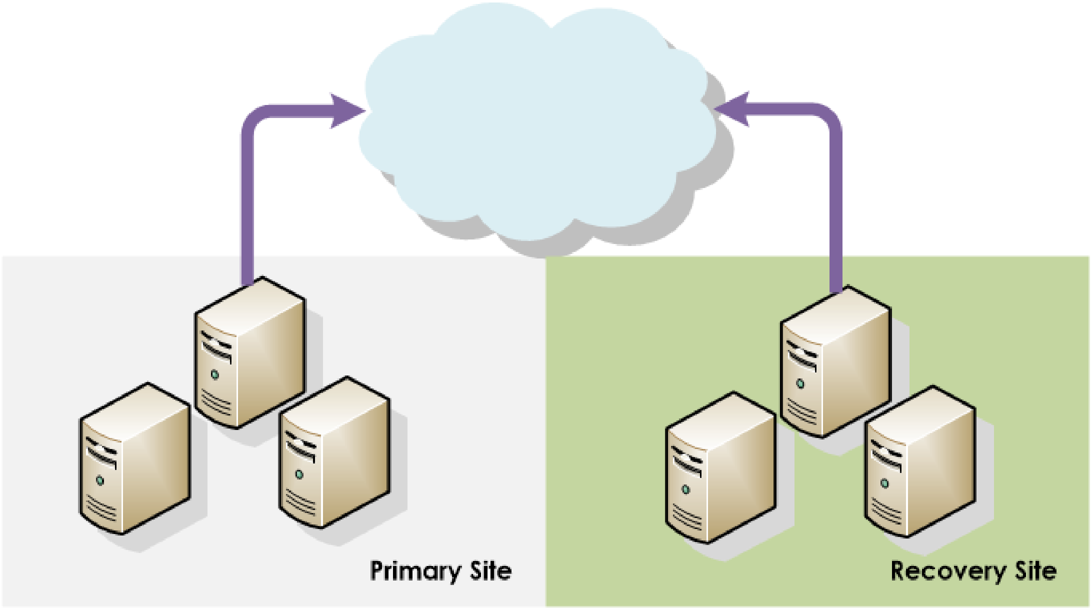
Hot site

- Fully redundant equipment
- Network connectivity is enabled
- Failover occurs within hours or days
- Near real-time data synchronization
- Zero data loss
- Expensive

- **Hot Sites:** Fully configured computer facility with all services
- **Warm Sites:** Like hot site, but software applications not kept fully prepared
- **Cold Sites:** Only rudimentary services and facilities kept in readiness

Business Continuity Plan (cont’d.)

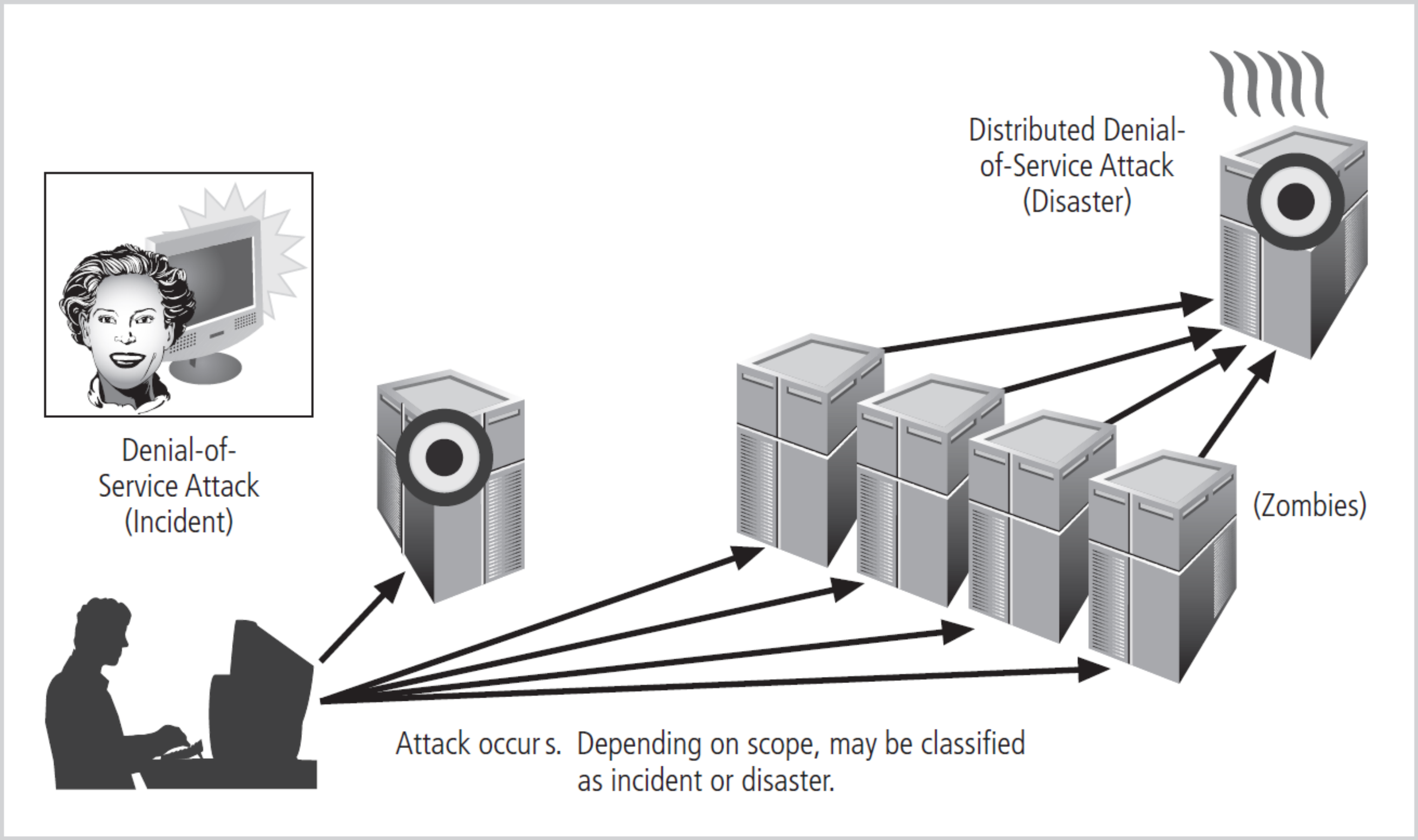
- **Timeshares:** Like an exclusive use site but leased
- **Service bureaus:** Agency that provides physical facilities
- **Mutual agreements:** Contract between two organizations to assist
- **Specialized alternatives**
  - ➢ Rolling mobile site
  - ➢ Externally stored resources



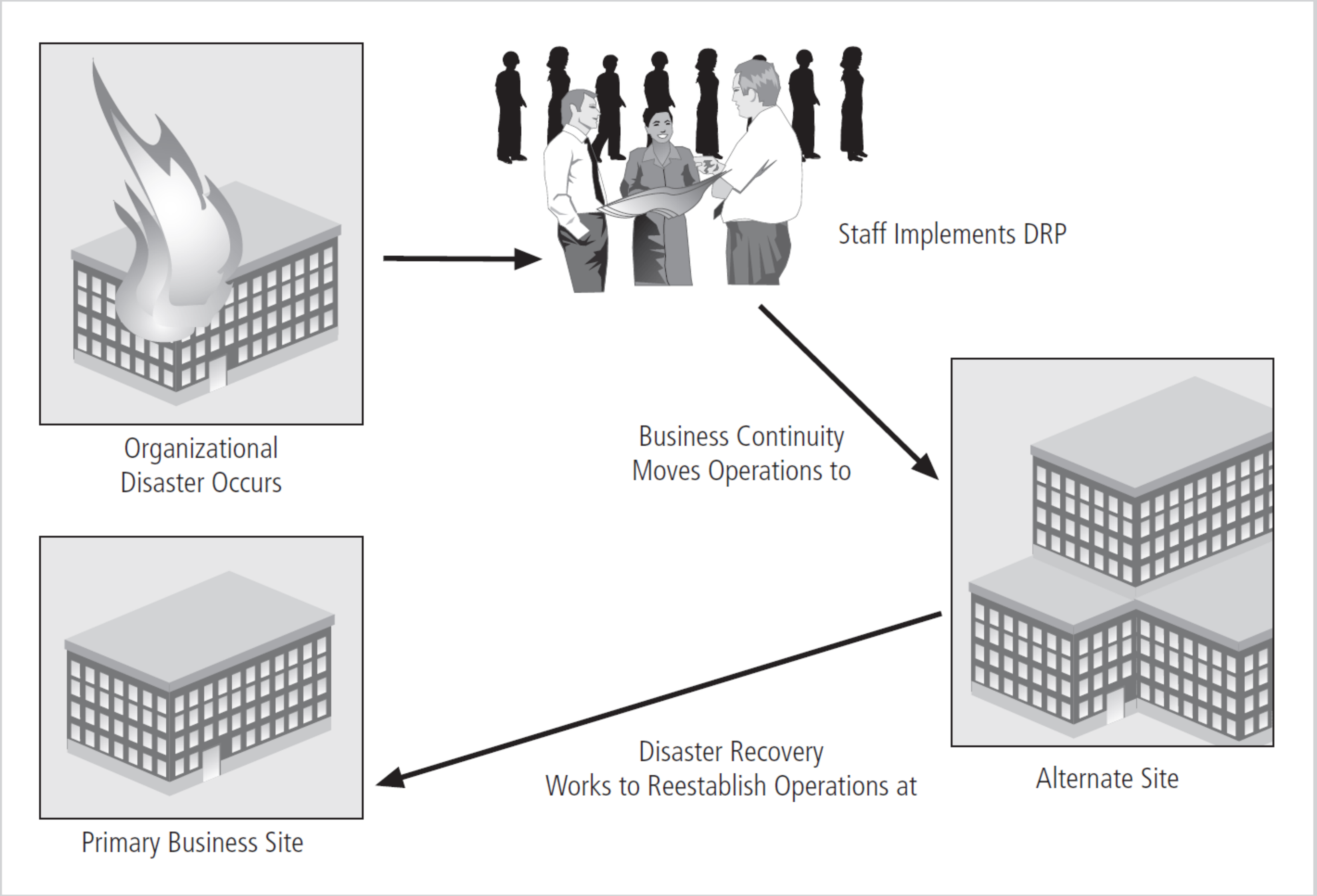
Data Backups

- To get any BCP site running quickly organization must be able to recover data
- Options include:
  - Traditional data backups
  - Electronic vaulting: Bulk batch-transfer of data to an off-site facility
  - Remote journaling: Transfer of live transactions to an off-site facility
  - Database shadowing: Storage of duplicate online transaction data

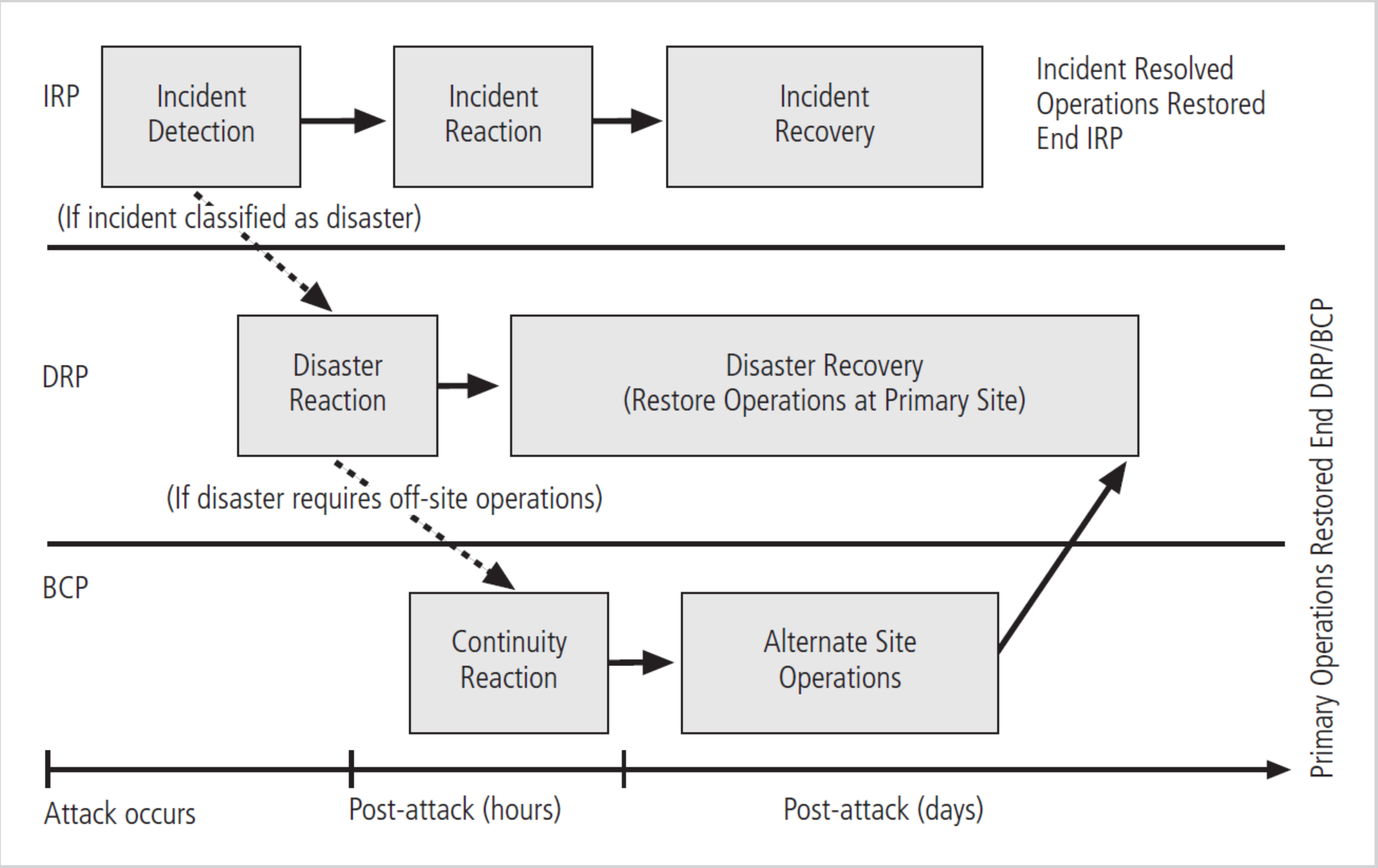
Timing and Sequence of CP Elements



Timing and Sequence of CP Elements (cont'd.)



Timing and Sequence of CP Elements (cont’d.)



Testing Contingency Plans

- Problems are identified during testing
  - ➢ Improvements can be made, resulting in a reliable plan

- Contingency plan testing strategies
  - ➢ Desk check
  - ➢ Structured walkthrough
  - ➢ Simulation
  - ➢ Parallel testing
  - ➢ Full interruption testing

Contingency Planning: Final Thoughts

- Iteration results in improvement
- A formal implementation of this methodology is a process known as continuous process improvement (CPI)
- Each time the plan is rehearsed it should be improved
- Constant evaluation and improvement lead to an improved outcome