

Information Security

CS 3002

Dr. Haroon Mahmood

Assistant Professor

NUCES Lahore

Security Planning

- The process of creating information security program includes:
 - Create *policies, standards, and practices*
 - Design of information security architecture
 - Use of a detailed information security mechanism
 - Creation of *contingency planning* consisting of incident response planning, disaster recovery planning, and business continuity plans
- Without policy, blueprints, and planning, organization is unable to meet information security needs of various communities of interest

Security Policy

- Organizations must consider policies as basis for all information security efforts
- Policies direct how issues should be addressed and technologies used
 - Security Plan and associated course of action
 - Convey instructions to ensure Security and Privacy
 - Create Organizational laws
 - Dictate acceptable and unacceptable behavior
 - Define penalties for violating policy
- **Security Policy** – set of rules that protects and organization's assets

Security Policy

- Security policies are least expensive controls to execute but most difficult to implement
- Shaping policy is difficult it should...
 - Never conflict with laws
 - Standup in court if challenged
- For a policy to be effective, must be properly disseminated, read, understood and agreed to by all members of organization

Standards

- **Detail statements of what must be done to comply with policy**

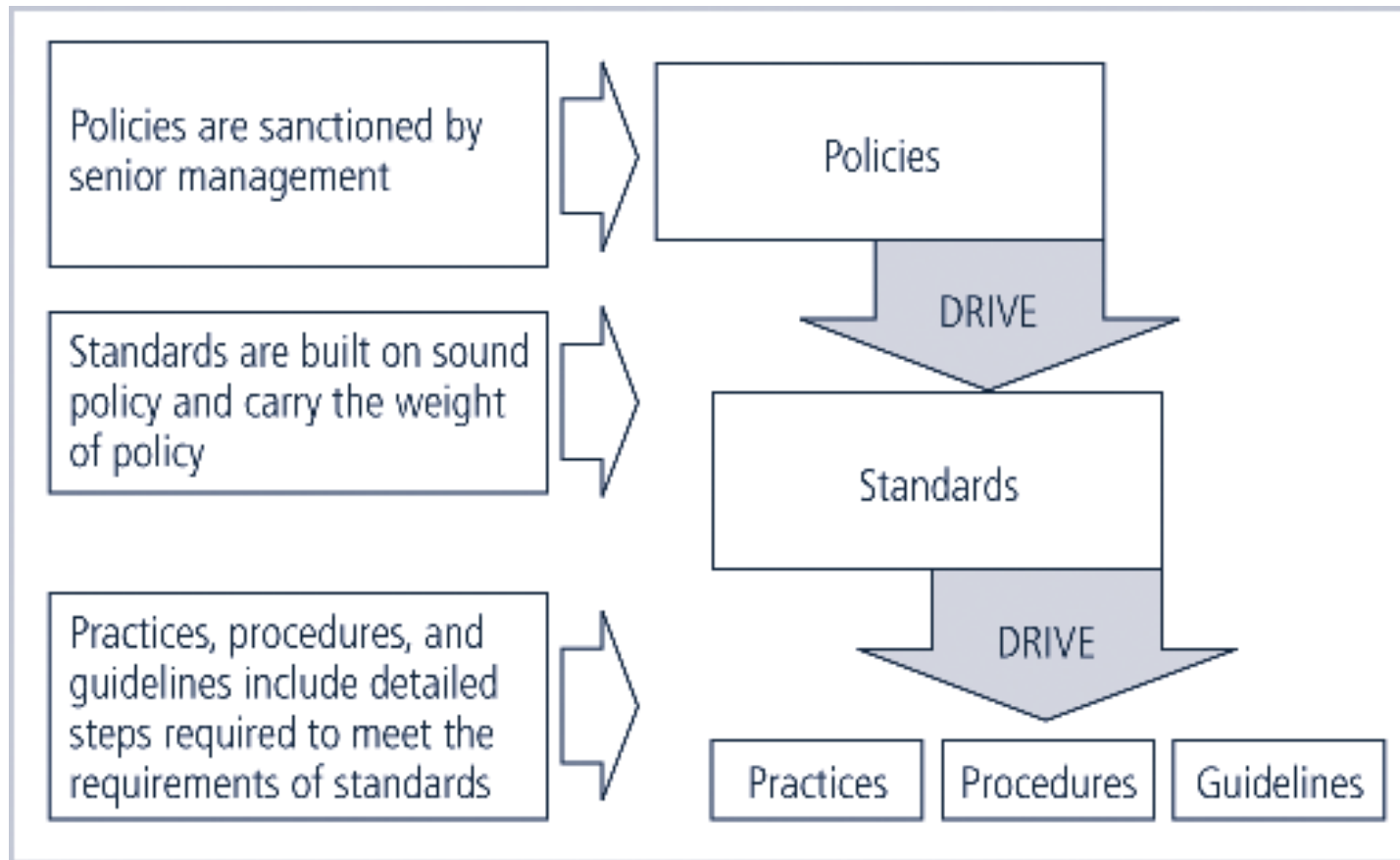


FIGURE 5-1 Policies, Standards, and Practices

Security Framework: Spheres of Security

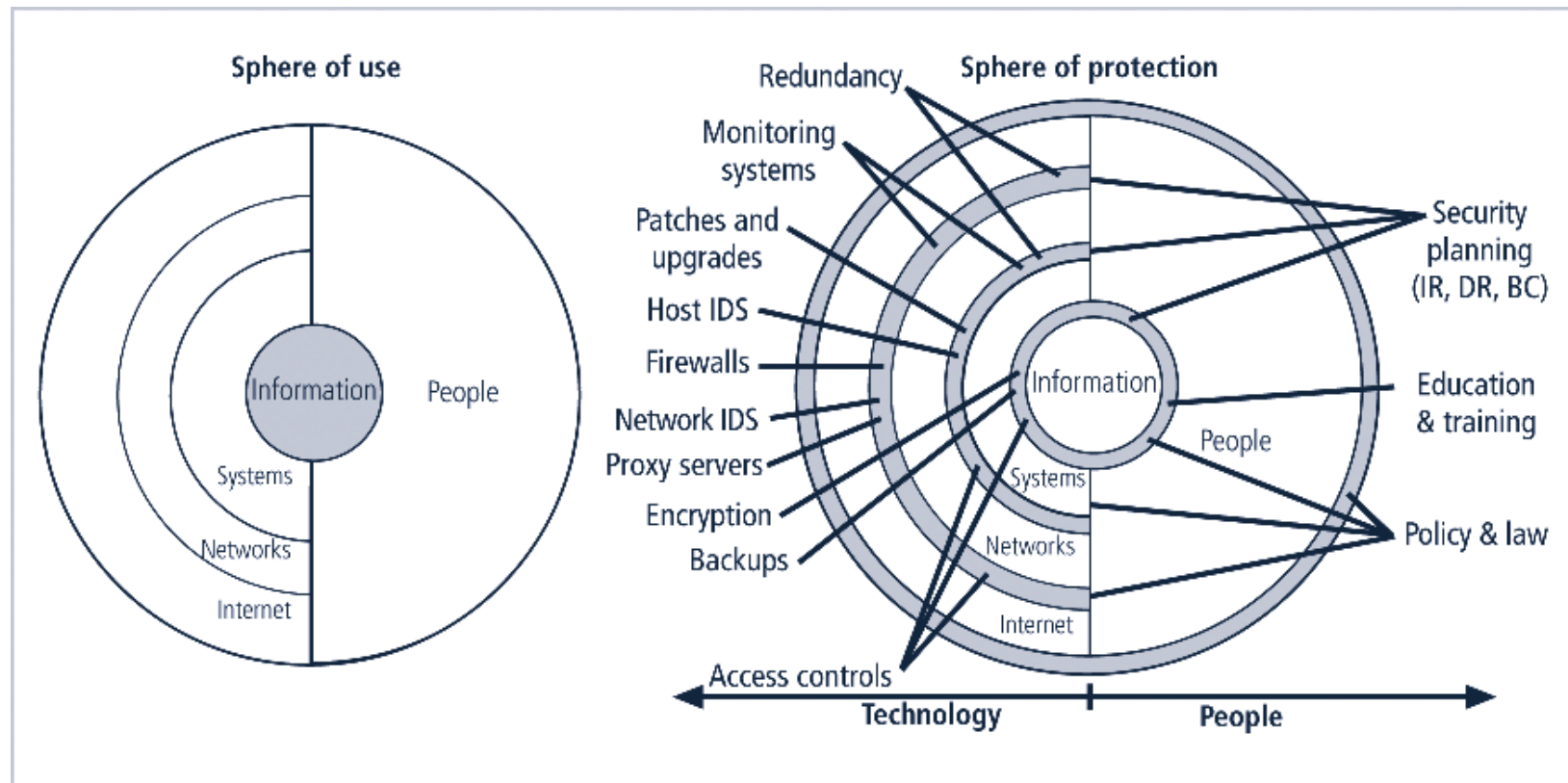


FIGURE 5-15 Spheres of Security

Risk Control Strategies

- **Four strategies to control security risks:**
 - **Apply safeguards that eliminate or reduce residual risks (avoidance)**
 - **Transfer the risk to other areas or outside entities (transference)**
 - **Reduce the impact should the vulnerability be exploited (mitigation)**
 - **Understand the consequences and accept the risk without control or mitigation (acceptance)**

Avoidance Strategies

- Attempts to prevent exploitation of the vulnerability
- Preferred approach; accomplished through countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards
- Three common methods of risk avoidance:
 - Application of policy
 - Training and education
 - Applying technology

Transference

- **Control approach that attempts to shift risk to other assets, processes, or organizations**
 - Rethinking how services are offered
 - Revising deployment models
 - Outsourcing
 - Purchasing insurance
 - Implementing service contracts
- **In Search of Excellence**
 - Concentrate on what you do best

Acceptance

- ***Doing nothing*** to protect a vulnerability and accepting the outcome of its exploitation
- Valid only when the particular function, service, information, or asset does not justify cost of protection
- ***Risk appetite*** describes the degree to which organization is willing to accept risk as trade-off to the expense of applying controls

Mitigation

- **Attempts to reduce impact of vulnerability exploitation through planning and preparation**
- **Approach includes three types of plans:**
 - **Incident response plan (IRP)**
 - **Disaster recovery plan (DRP)**
 - **Business continuity plan (BCP)**

Mitigation

- **Disaster recovery plan (DRP) is most common mitigation procedure**
- **The actions to take while incident is in progress is defined in Incident response plan (IRP)**
- **Business continuity plan (BCP) encompasses continuation of business activities if catastrophic event occurs**

Contingency Planning

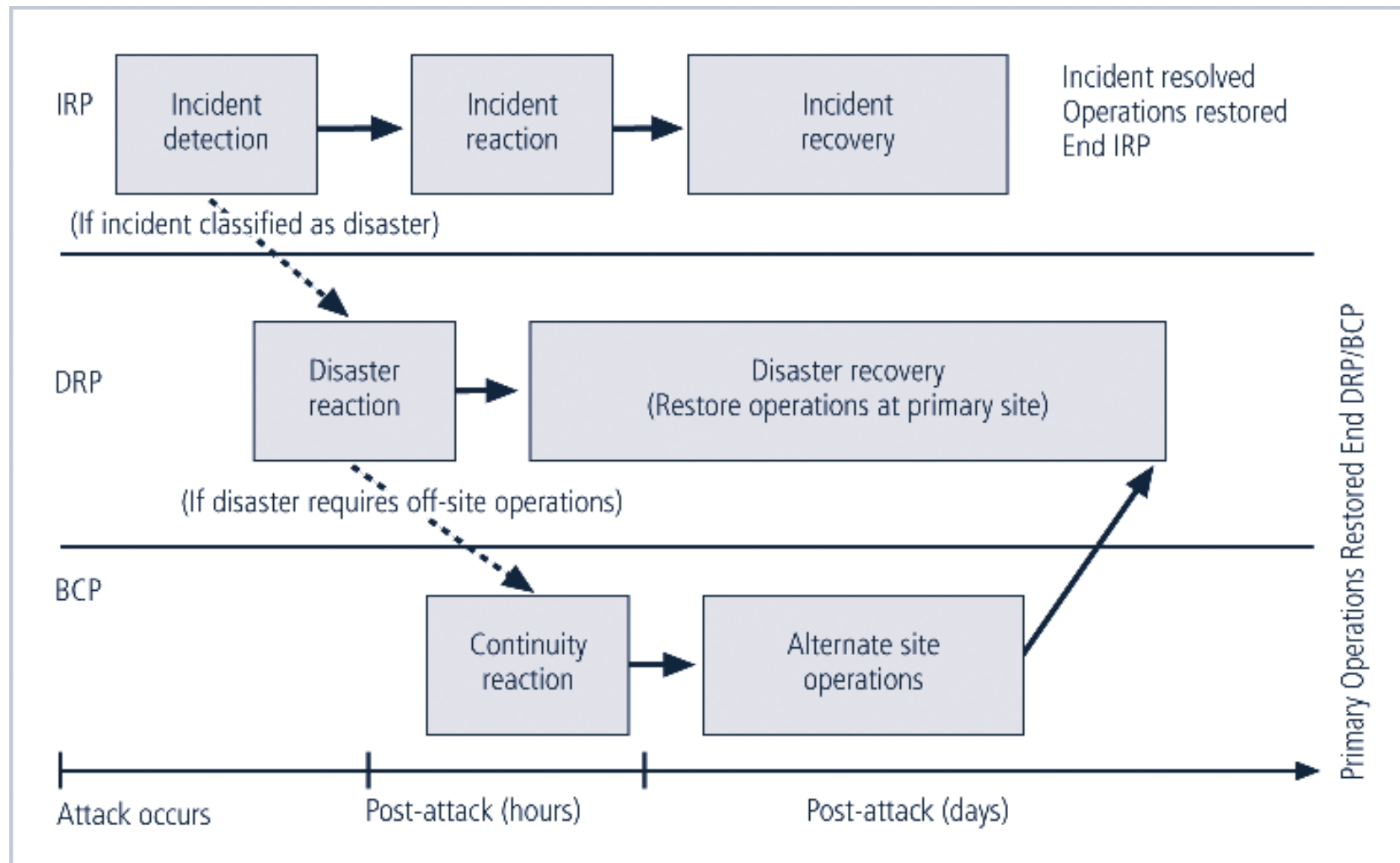


FIGURE 5-22 Contingency Planning Timeline

Steps of Contingency planning

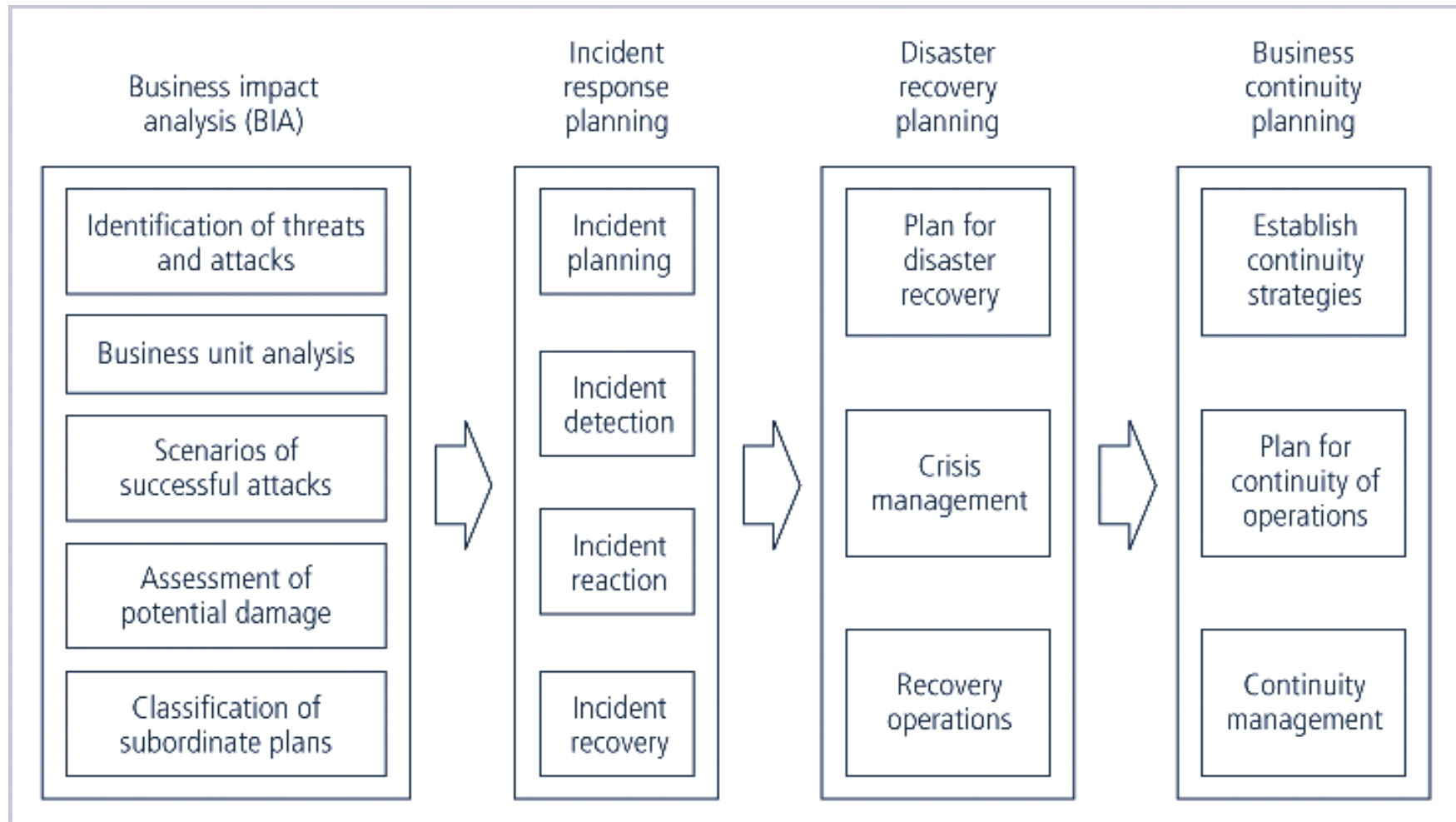


FIGURE 5-23 Major Steps in Contingency Planning

Incident Response Planning (IRPs)

- Incident response planning covers identification of, classification of, and response to an incident
- Attacks classified as incidents if they:
 - Are directed against information assets
 - Have a realistic chance of success
 - Could threaten confidentiality, integrity, or availability of information resources
- Incident response (IR) is more reactive, than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident

Incident response

- **Set of activities taken to plan for, detect, and correct the impact**
- **Incident planning**
 - Requires understanding BIA scenarios
 - Develop series of predefined responses
 - Enables org to react quickly
- **Incident detection**
 - Mechanisms – intrusion detection systems, virus detection, system administrators, end users

Incident detection

- **Possible indicators**
 - Presence of unfamiliar files
 - 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

Incident detection

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

- **Predefined Situation**
 - Loss of availability
 - Loss of integrity
 - Loss of confidentiality
 - Violation of policy
 - Violation of law

Incident reaction

- **Actions outlined in the IRP**
- **Guide the organization**
 - **Stop the incident**
 - **Mitigate the impact**
 - **Provide information recovery**
- **Notify key personnel**
- **Document incident**

Incident Containment Strategies

- **Sever affected communication circuits**
- **Disable accounts**
- **Reconfigure firewall**
- **Disable process or service**
- **Take down email**
- **Stop all computers and network devices**
- **Isolate affected channels, processes, services, or computers**

Incident Recovery

- **Get everyone moving and focused**
- **Assess Damage**
- **Recovery**
 - **Identify and resolve vulnerabilities**
 - **Address safeguards**
 - **Evaluate monitoring capabilities**
 - **Restore data from backups**
 - **Restore process and services**
 - **Continuously monitor system**
 - **Restore confidence**