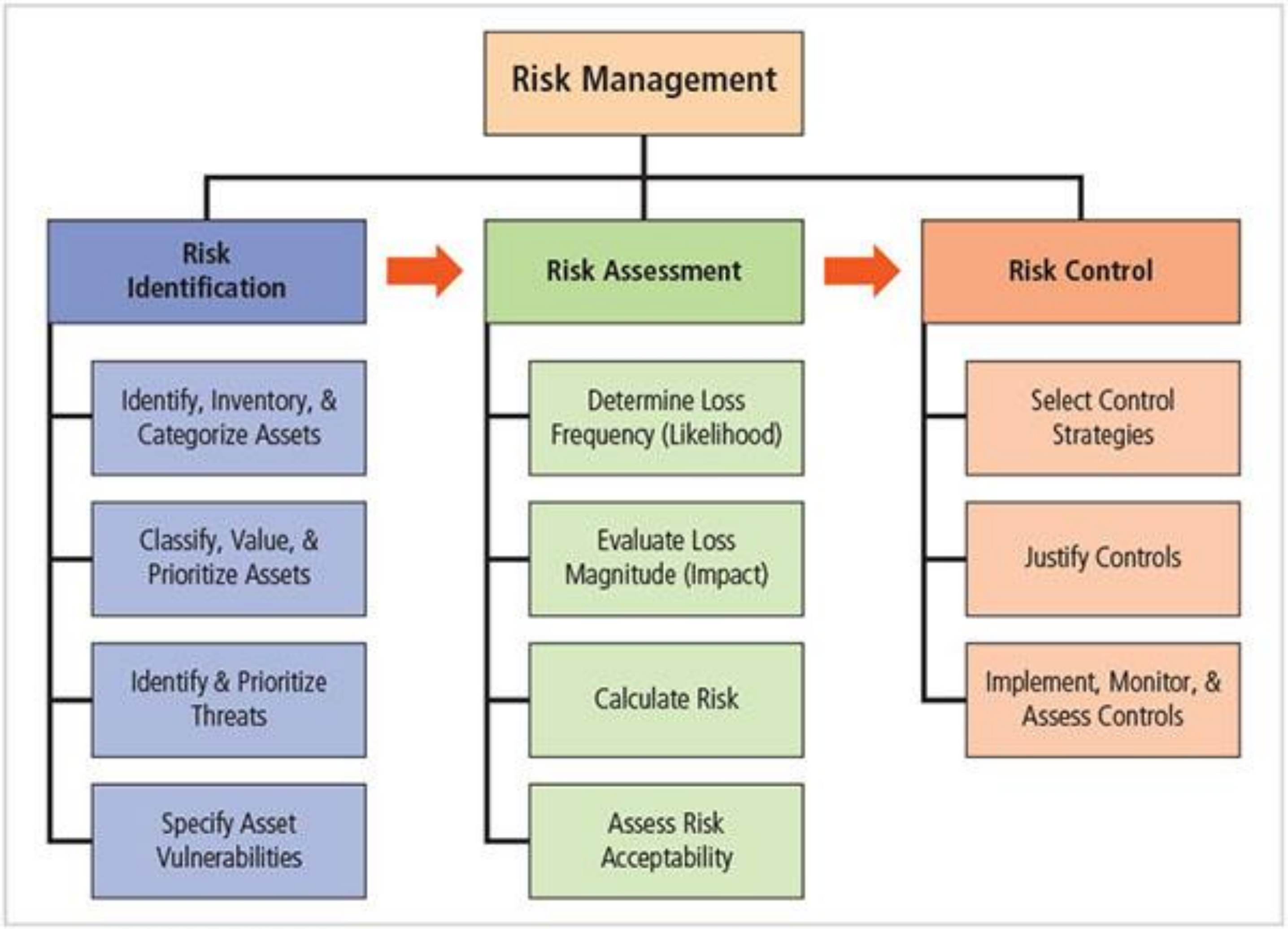
Dr. Ammar Haider
Assistant Professor
School of Computing

CS3002 Information Security

Risk Assessment and Management

Source: Whitman chap. 5

Risk Management



Risk Management

- Risk Identification
  - Identify, Inventory, & Categorize Assets
  - Classify, Value, & Prioritize Assets
  - Identify & Prioritize Threats
  - Specify Asset Vulnerabilities
- Risk Assessment
  - Determine Loss Frequency (Likelihood)
  - Evaluate Loss Magnitude (Impact)
  - Calculate Risk
  - Assess Risk Acceptability
- Risk Control
  - Select Control Strategies
  - Justify Controls
  - Implement, Monitor, & Assess Controls

Figure 5-1

Risk Likelihood

- Chances that the organization will have to face a specific threat
- Could be expressed as low, moderate high, or as a probability 0–1
- Can be estimated from organization history or published studies

Loss Magnitude (Impact)

- How much is the effect on organization business when risk occurs
- What percentage of asset value will be lost in the attack
- Again can be expresses as low, moderate, high or as a number on an arbitrary scale (say 1–10)

Calculate Risk Score

Risk Element	Likelihood	Impact/Cost	Score likelihood × impact	Controls
Exploiting vulnerability in application server				
SQLi attack on database server				
A junior employee’s password stolen				
DDoS attack on website				
Ransomware attack on org				
Staff members ill				
Internet down for couple hours				
Major flood				

Risk Control Strategies

- **Defense** – Apply safeguards that eliminate or reduce the residual risk
- **Transference** – Transfer the risk to other areas or outside entities
- **Mitigation** – Reduce the impact should the vulnerability be exploited
- **Acceptance** – Understand the consequences and accept the rest without mitigation
- **Termination** – avoid business activities that introduce an uncontrollable risk

Defense

Attempts to prevent the exploitation of the vulnerability

- Reduce the likelihood of attack
- Preferred approach

Accomplished through:

- countering threats
- removing asset vulnerabilities
- limiting asset access
- adding protective safeguards

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 attack (rather than likelihood of attack) through planning and preparation

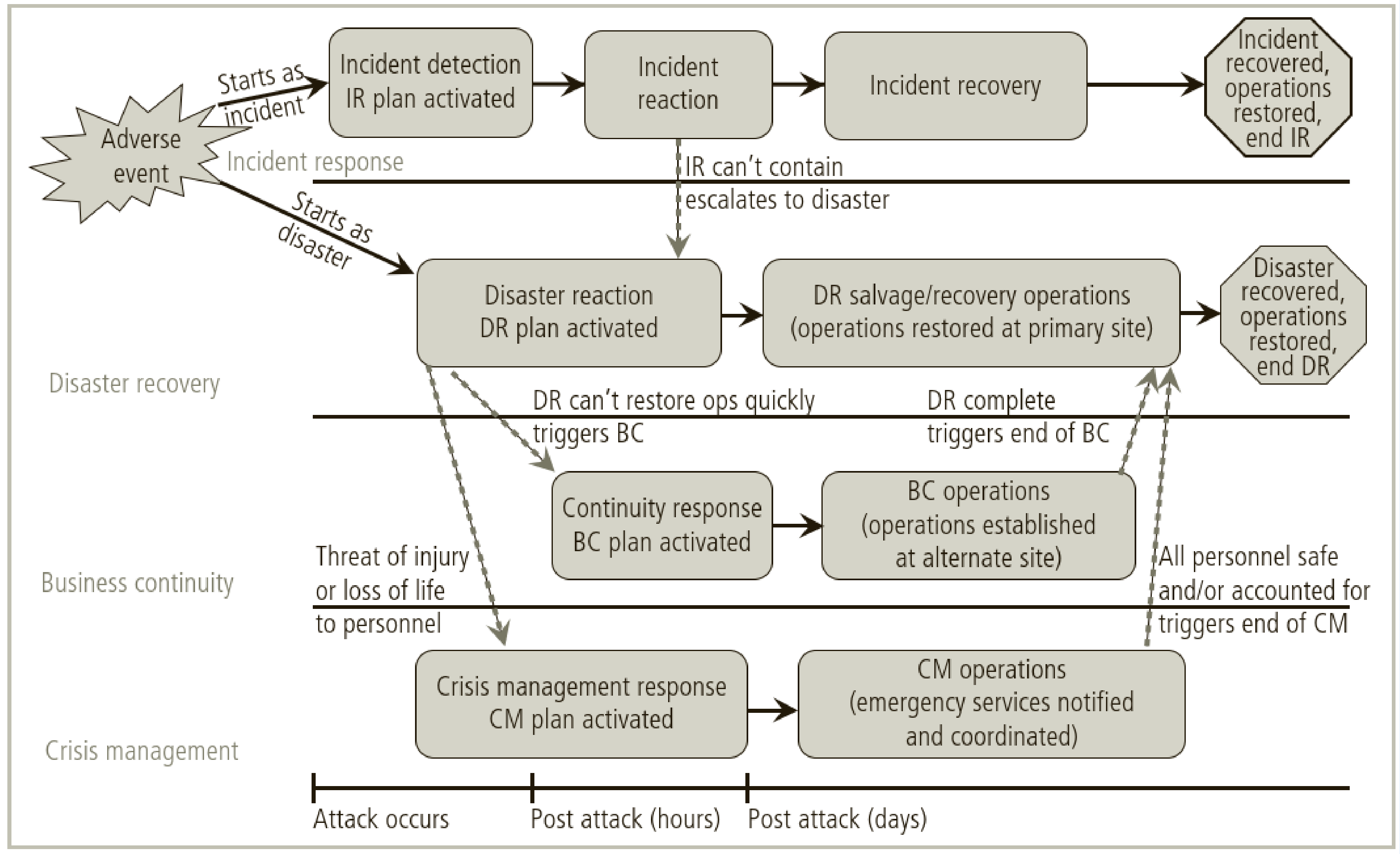
It includes three types of contingency plans:

- Incident Response Plan (IRP): The actions to take immediately while incident is in progress
- Disaster Recovery Plan (DRP): includes preparation for the recovery, strategies to limit losses, steps to follow in the aftermath
- Business Continuity Plan (BCP): encompasses continuation of business activities if catastrophic event occurs

Contingency Planning

Whitman chap. 4

Contingency Planning Timeline


Adverse event
Starts as incident
Incident detection IR plan activated
Incident reaction
Incident recovery
Incident recovered, operations restored, end IR
Incident response
IR can't contain escalates to disaster
Starts as disaster
Disaster reaction DR plan activated
DR salvage/recovery operations (operations restored at primary site)
Disaster recovered, operations restored, end DR
Disaster recovery
DR can't restore ops quickly triggers BC
DR complete triggers end of BC
Continuity response BC plan activated
BC operations (operations established at alternate site)
Business continuity
Threat of injury or loss of life to personnel
All personnel safe and/or accounted for triggers end of CM
Crisis management response CM plan activated
CM operations (emergency services notified and coordinated)
Crisis management
Attack occurs
Post attack (hours)
Post attack (days)

Incident Response Planning

- Incident response planning covers identification and classification of an incident and response to it

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, except for planning that must occur to prepare IR teams to be ready to react to an incident

Incident Response Planning

- Develop a series of predefined responses
  - Set of activities taken to detect and correct the impact
  - Enables organization 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 form 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 incident situations

- 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 if possible
- Disable accounts
- Reconfigure firewall
- Disable process or service
- Take down email
- Isolate affected channels, processes, services, or computers
- Most drastic: Stop all computers and network devices

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

Disaster Recovery Plan (DRP)

- Provide guidance in the event of a disaster
- **Aim**: Secure most valuable assets, at the risk of short term disruption.
- Clear establishment of priorities
- Clear delegation of roles & responsibilities
- Alert key personnel
- Document disaster
- Mitigate impact
- Evacuation of physical assets