LECTURE 13
CONTINGENCY PLAN

Dr Warusia Mohamed Yassin

Topics

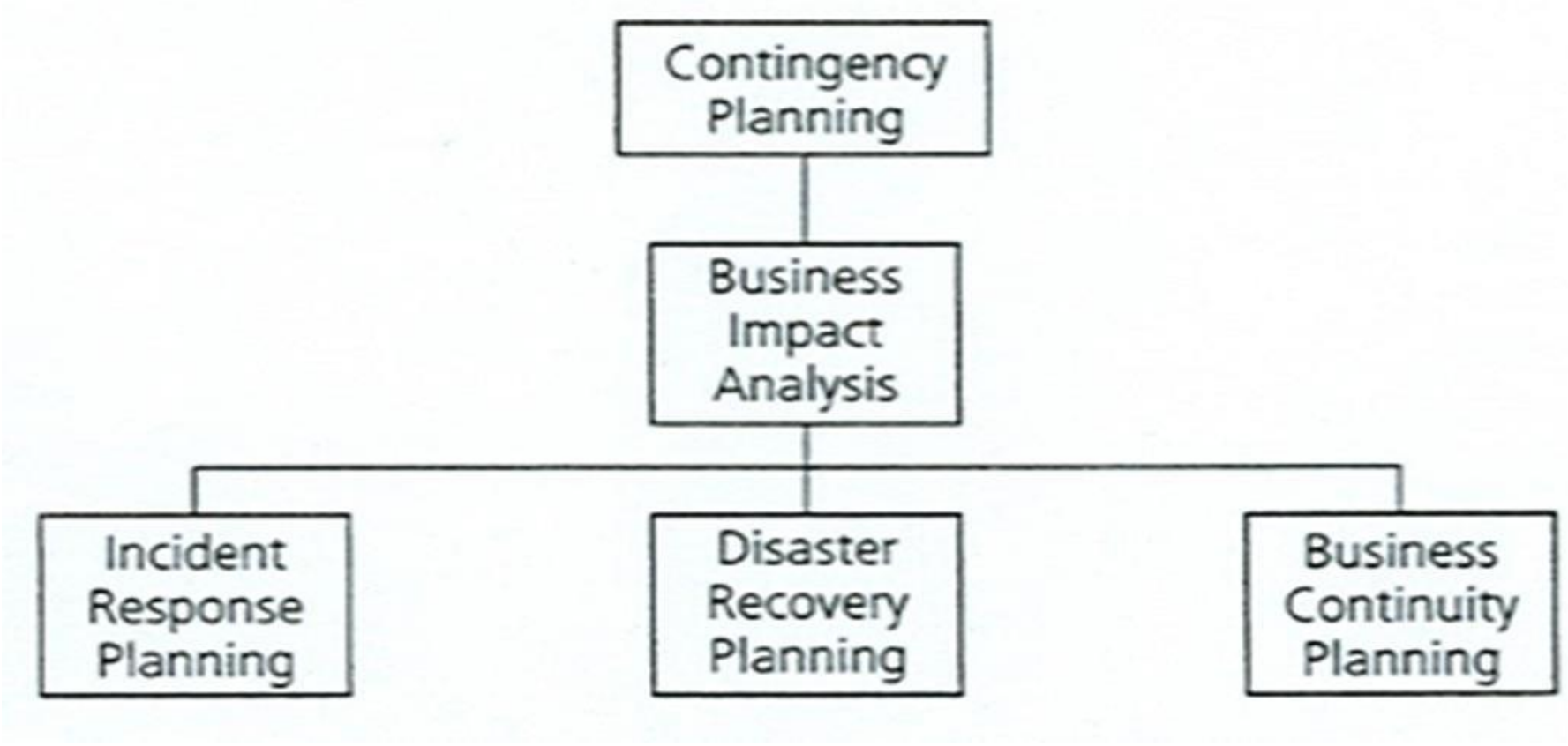
- Contingency Plan
- Business Impact Analysis
- Disaster Recovery Plan
- Business Continuity Plan
- Backup

What is Contingency Plan?

- ✓ The overall process of preparing for unexpected events
- ✓ Prepare for, detect, react to, recover from these events

"many organization contingency plans are woefully inadequate…"

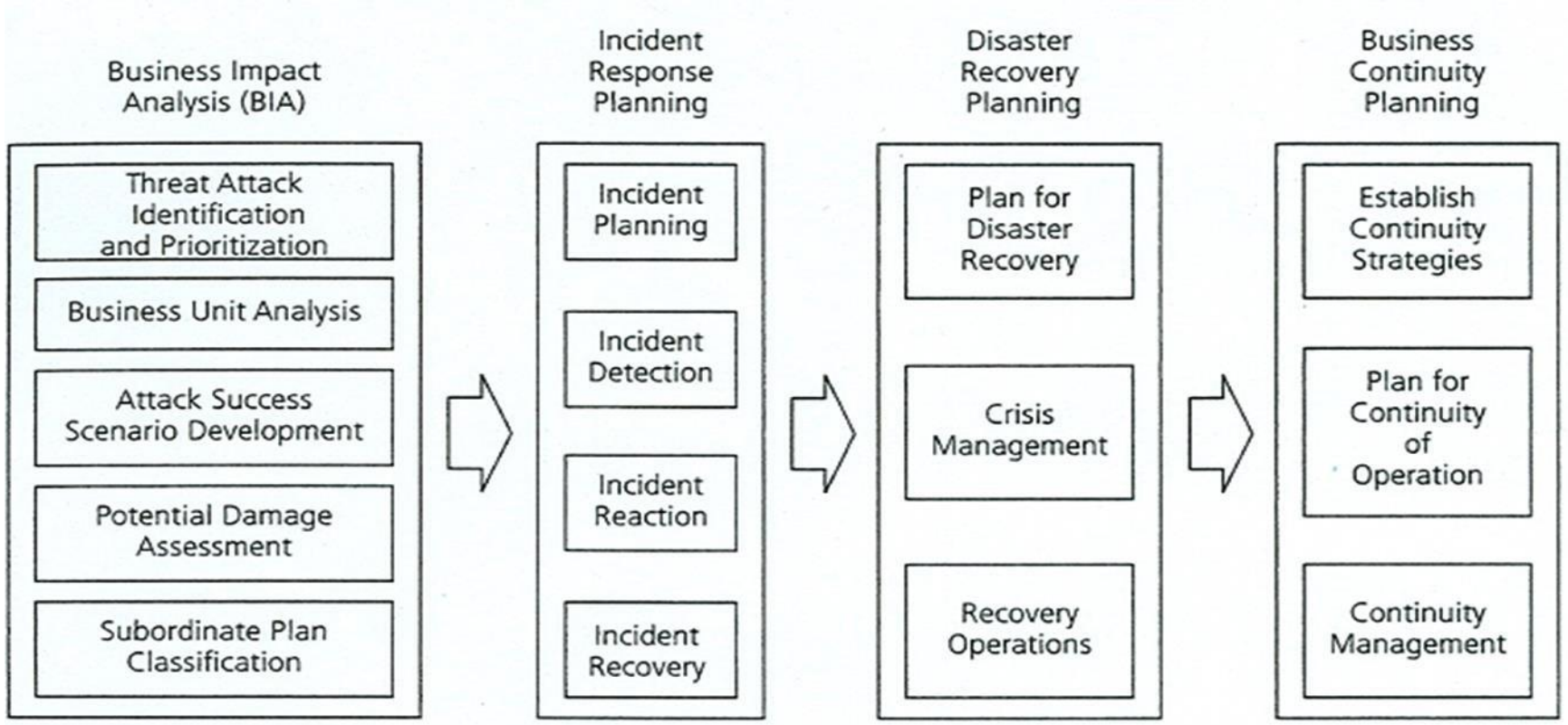
Component of Contingency Plan



Component of Contingency Plan

- ✓ Business Impact Analysis (BIA)
  - ✓ Determine critical business functions and information systems
- ✓ Incident Response Plan (IR)
  - ✓ Immediate response to an incident
- ✓ Disaster Recovery Plan (DR)
  - ✓ Focus on restoring operations at the primary site
- ✓ Business Continuity Plan (BC)
  - ✓ Enables business to continue at an alternate site
  - ✓ Occurs concurrently with DR Plan

Component of Contingency Plan (Detail Task)



Business Impact Analysis

- ✓ Provides detailed scenarios of effects of potential attacks
- ✓ Risk management identifies attacks
- ✓ BIA assumes controls have failed

Disaster Recovery Plan (DRP)

- ✓ Entails the preparation for and recovery from a disaster
- ✓ Responsibility of the IT community of interest, under the leadership of the CEO
- ✓ An incident becomes a disaster when
  - ✓ The organization is unable to contain or control the impact of an incident
  - ✓ The level of damage is so severe that the organization cannot recover from the incident

The key role of a DR plan is to reestablish operations at the primary location

DRP Process

1. Develop the DR planning policy statement
2. Review the BIA
3. Identify preventive controls
4. Develop recovery strategies
5. Develop the DR plan document
6. Plan testing, training and exercises
7. Plan maintenance

Classification of Disaster

- ✓ Natural disasters
  - ✓ Examples: Fire, flood, hurricane, tornado
- ✓ Man-made disasters
  - ✓ Examples: Cyber-terrorism
- ✓ Rapid-onset
  - ✓ Examples: Earthquakes, mud-flows
- ✓ Slow-onset
  - ✓ Examples: Famines, deforestation

Business Continuity Plan (BCP)

- ✓ Ensures that critical business functions can continue if a disaster occurs
- ✓ CEO should manage
- ✓ Activated and executed concurrently with DR plan
  - ✓ Business can no longer function at primary location
  - ✓ Use an alternate location
- ✓ Identify critical business functions and resources to support them
- ✓ Want to quickly re-establish these functions at alternate site

BCP Process

1. Develop the BC planning policy statement
   - Authority, guidance, executive vision
2. Review the BIA
   - Identify, prioritize critical IT systems
3. Identify preventive controls
   - Measures to reduce disruption, increase system availability
4. Develop relocation strategies
   - Critical systems must be recovered quickly
5. Develop the continuity plan
   - Include detailed guidelines and procedures
6. Plan testing, training, and exercises
   - Identify planning gaps, prepare personnel for improved effectiveness and preparedness
7. Plan maintenance
   - Living document, plan to update!

Final Thoughts

- ✓ Iteration results in improvement
- ✓ Each time the organization rehearses its plans, it must learn and improve
- ✓ Each time an incident or a disaster occurs the organization should review what went right and what went wrong
- ✓ Through ongoing evaluation and improvement an organization continually improves and strives for better outcomes
- ✓ Contingency planning and its various components BIA, IRP, DRP and BCP play a critical role in preparing for, detecting, reacting to and recovering from events that threaten the security of information resources and assets both human and natural.

Roadmap/Mind Map