GJØVIK UNIVERSITY COLLEGE

Security Planning and Incident Management

Marie Moe, NSM/HiG

Gjøvik 28.04.14

AGENDA

Project Work Evaluation

- *Peer reviews*
- *Generic feedback*

Disaster Recovery and Business Continuity

- *Preparation & Implementation*
  - *Forming the DR and BC teams*
  - *Key functions in a DR/BC plan*
- *Operation & Maintenance*
  - *Critical elements in the response phase*
  - *How to resume normal operations*

PROJECT WORK EVALUATION

Peer reviews

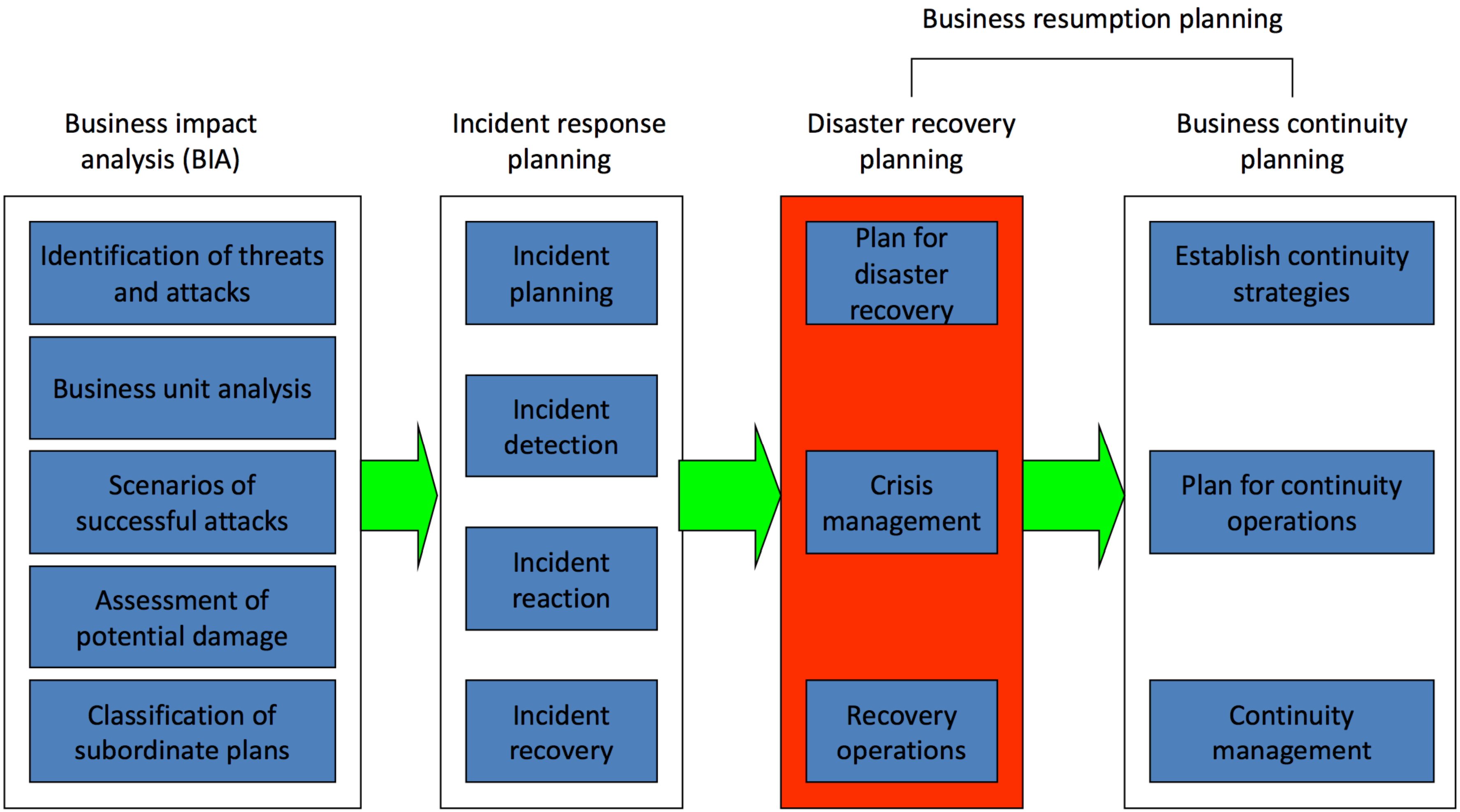
- A document with names of who is going to peer review each others work has been published on Fronter
- Get in touch with the other student/group and exchange your drafts
- Your evaluation is then submitted to the other student/group, not the lecturer

The project work submission deadline has been extended to the 16th of May!

PROJECT WORK EVALUATION

Generic feedback

- Remember your audience!
- The introduction and the conclusion is very important
- Correct grammar mistakes and spelling errors
- Remember to refer to a figure/table in the text
- Also explain figures/tables
- Do not forget references for figures that are reproduced


Business resumption planning
Business impact analysis (BIA)
Identification of threats and attacks
Business unit analysis
Scenarios of successful attacks
Assessment of potential damage
Classification of subordinate plans
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 operations
Continuity management

Whitman and Mattord 2007, p. 27

WHY DO WE NEED DISASTER RECOVERY PLANS?

- Over 90 percent of those organizations experiencing disruptions at a data center lasting 10 days or longer were forced into bankruptcy within a year
- Over 40 percent of the companies that experience a disaster never reopen
- Nearly 30 percent of companies that experience a disaster fail within 2 years
- Downtime as a function of labor exposes large organizations to an average loss of 1 million USD per hour

Whitman, Mattord and Green 2014, p. 371

DISASTER CLASSIFICATIONS

- **Natural** disasters vs **man-made** disasters
  - Man-made disasters:
    - *Terrorism*
    - *Acts of war*
    - *Incidents that escalate to disasters*
  - Natural disasters:
    - *Fire, flood, earthquake, tsunami, …*
    - *Electrostatic discharge, dust contamination, excessive precipitation*

- **Rapid-onset** disasters vs **slow-onset** disasters

FORMING THE DISASTER RECOVERY TEAM

- Team leader and representatives from every major org. unit:
  - Senior management
  - Corporate support units
  - Facilities
  - Fire and safety
  - Maintenance
  - IT technical staff
  - InfoSec technicians and managers
- There should be no overlap with IR and BC team members!

Whitman, Mattord and Green 2014, p. 373-374

DISASTER RECOVERY SUBTEAMS

- Disaster Management Team
- Communications Team
- Computer Recovery (Hardware) Team
- Systems Recovery (OS) Team
- Network Recovery Team
- Storage Recovery Team
- Applications Recovery Team
- Data Management Team
- Vendor Contact Team
- Damage Assessment And Salvage Team
- Business Interface Team
- Logistics Team
- Other teams as needed…

DR: SPECIAL DOCUMENTATION AND EQUIPMENT

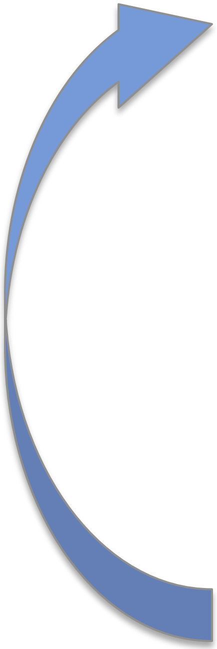
Each member of the DR team should have multiple copies of the DR and BC plans in their homes, vehicles and offices

- *Be aware that this may be a security risk and that appropriate steps should be taken to ensure the information does not fall into the wrong hands!*

Other equipment:

- Data recovery software
- Redundant hardware and components
- Copies of building blueprints with important locations highlighted
- Key phone numbers
- Emergency supplies

THE SEVEN STEP CONTINGENCY PLANNING PROCESS

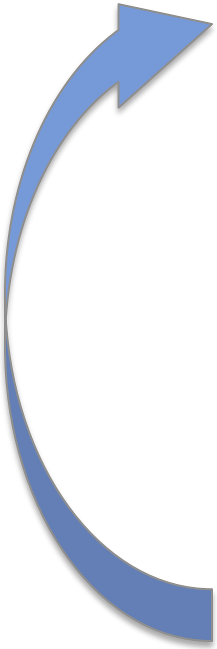


1. Develop the contingency planning policy
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. Ensure plan maintenance

M. Swanson, P. Bowen, A. Phillips, D. Gallup and D. Lynes, ”Contingency Planning Guide for Federal Information Systems”, NIST Special Publication 800-34 Rev. 1, accessed February 2014 from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Also see Whitman and Mattord 2007 p. 51 or Whitman, Mattord and Green 2014 p. 53

THE SEVEN STEP CONTINGENCY PLANNING PROCESS ADAPTED TO DISASTER RECOVERY (DR)



1. Develop the DR policy
2. Review the business impact analysis (BIA)
3. Identify preventive controls
4. Create DR contingency strategies
5. Develop the DR plan
6. Ensure DR plan testing, training, and exercises
7. Ensure DR plan maintenance

Whitman, Mattord and Green 2014 p. 377-378

DEVELOP RECOVERY STRATEGIES

- Should cover most expected disasters
  - Based on the BIA

- After the action actions
  - Processes for technical data backup and recovery
  - Steps to fully restore the organisation to its operational status
  - *Must be thoroughly developed and tested*

- It may be helpful to involve contractors in DR training and rehearsals

DR PLANNING: DURING THE DISASTER

- Specify triggers based on disaster scenarios
- Specify reaction strategies and procedures
- Hurricane example:
  - Warn employees not to come to work
  - Direct employees to shelters
- IT based disasters:
  - DR team works closely together with IR team to contain the incident that has escalated to a disaster

PLAN TRIGGERS AND NOTIFICATION

- Management notification
- Employee notification
- Emergency management notification
- Local emergency services
- Media outlets

KEY FEATURES OF THE DR PLAN

- Clear delegation of roles and responsibilities
- Execution of the alert roster and notification of key personnel
- Use of employee check-in systems
- Clear establishment and communication of business resumption priorities
- Complete and timely documentation of the disaster
- Preparations for alternative implementations

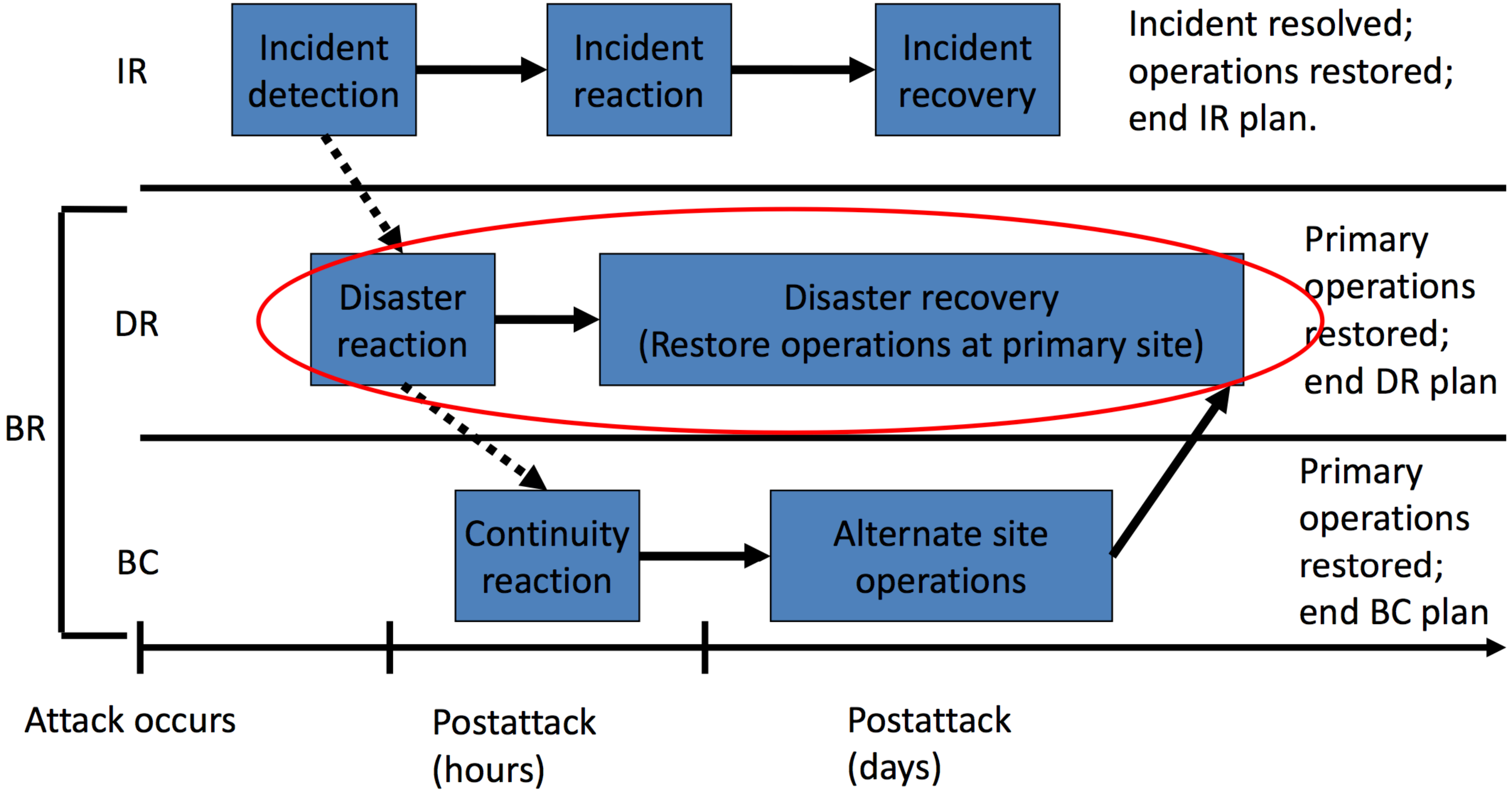
DR PLANNING: AFTER THE DISASTER

- Specify recovery strategies and procedures
- Identify potential follow on incidents and specify how to handle them
    - Forensic analysis
    - After-action review

DR PLANNING: BEFORE THE DISASTER

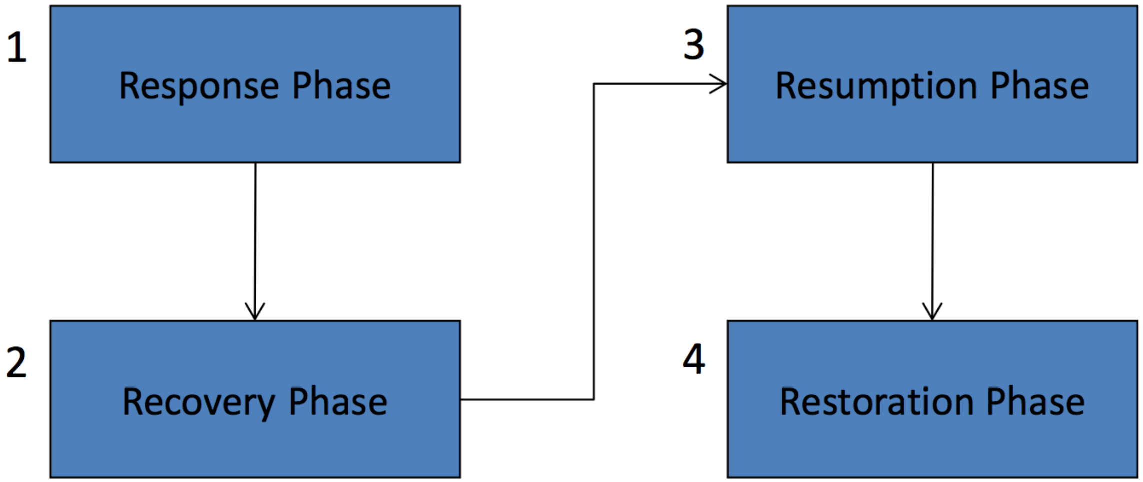
- Implement actions found in common information security practices
- Preventive security measures
- Enhancement of IR/DR/BC team preparedness
  - Training, stocking provisions, etc.
  - Cross-training employees could be useful
- Make sure off-site data and equipment storage locations are not knocked out by the same disaster!

CP: Timeline for Contingency Plan Execution


IR
Incident detection
Incident reaction
Incident recovery
Incident resolved; operations restored; end IR plan.
BR
DR
Disaster reaction
Disaster recovery (Restore operations at primary site)
Primary operations restored; end DR plan
BC
Continuity reaction
Alternate site operations
Primary operations restored; end BC plan
Attack occurs
Postattack (hours)
Postattack (days)

Whitman and Mattord 2007, p. 27

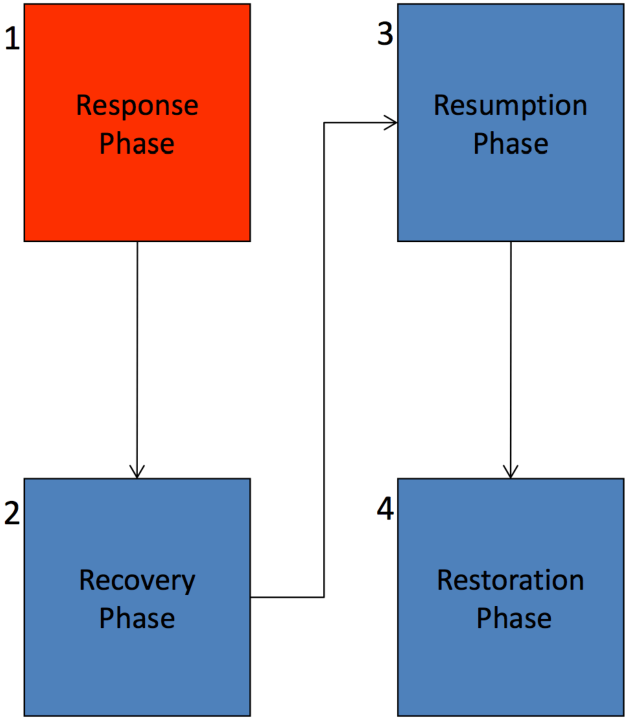
DISASTER RECOVERY PHASES



Based on M. Swanson, A. Wohl, L. Pope, T. Grance, J. Hash, R. Thomas, "Contingency Planning Guide for Information Technology Systems", NIST Special Publication 800-34, accessed June 13, 2005, from http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf. Also see Whitman and Mattord 2007, p. 316-327.

RESPONSE PHASE

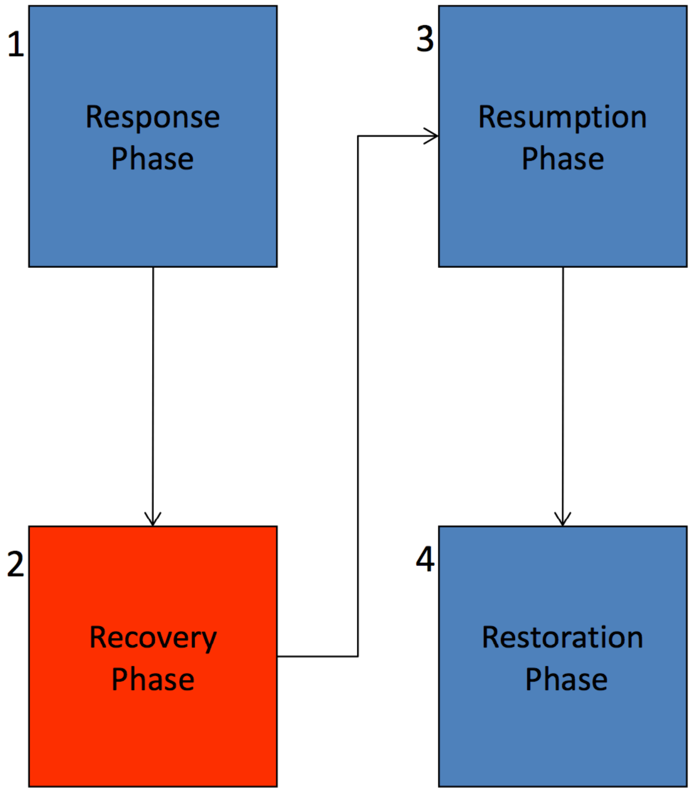
- Protect human life and well-being (physical safety)
- Attempt to limit and contain damage to the organisation’s facilities and equipment
- Manage communications with employees and other stakeholders



Whitman and Mattord 2007, p. 316-317

RECOVERY PHASE

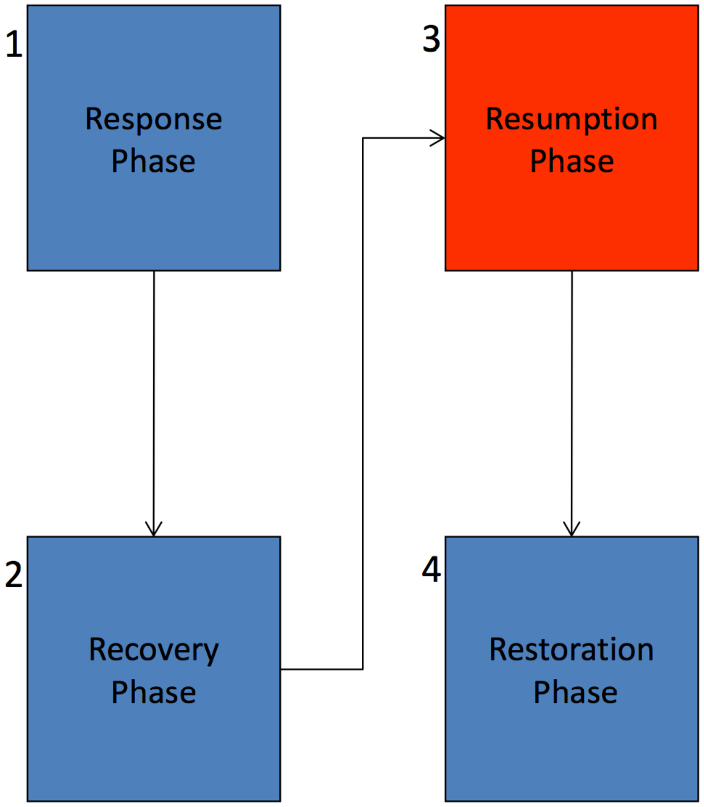
- Recover critical business functions
- Coordinate recovery efforts
- Acquire resources to replace damaged or destroyed materials and equipment
- Evaluate the need to implement the business continuity plan



Whitman and Mattord 2007, p. 318-319

RESUMPTION PHASE

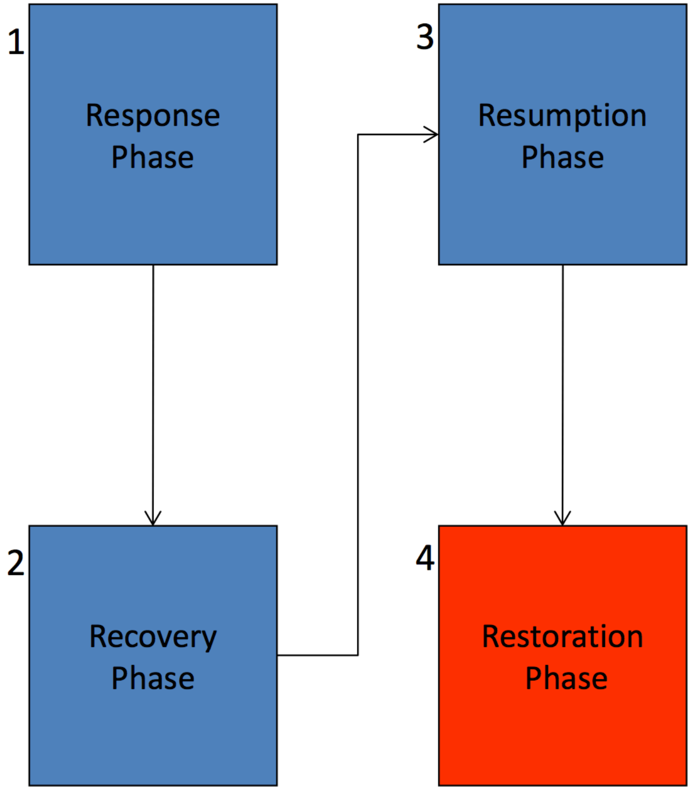
- Initiate implementation of secondary functions
- Finalize implementation of primary functions
- Identify additional needed resources
- Continue planning for restoration



Whitman and Mattord 2007, p. 320-321

RESTORATION PHASE

- Repair damage to the primary site or select or build a replacement facility
- Replace damaged or destroyed contents of the primary site
- Coordinate the relocation from temporary offices to the primary site or new replacement facility
- Restore normal operations at primary site, beggining with critical functions
- Stand down the DR team and conduct after action review



Whitman and Mattord 2007, p. 321-327

IT CONTINGENCY PLANNING RESOURCES

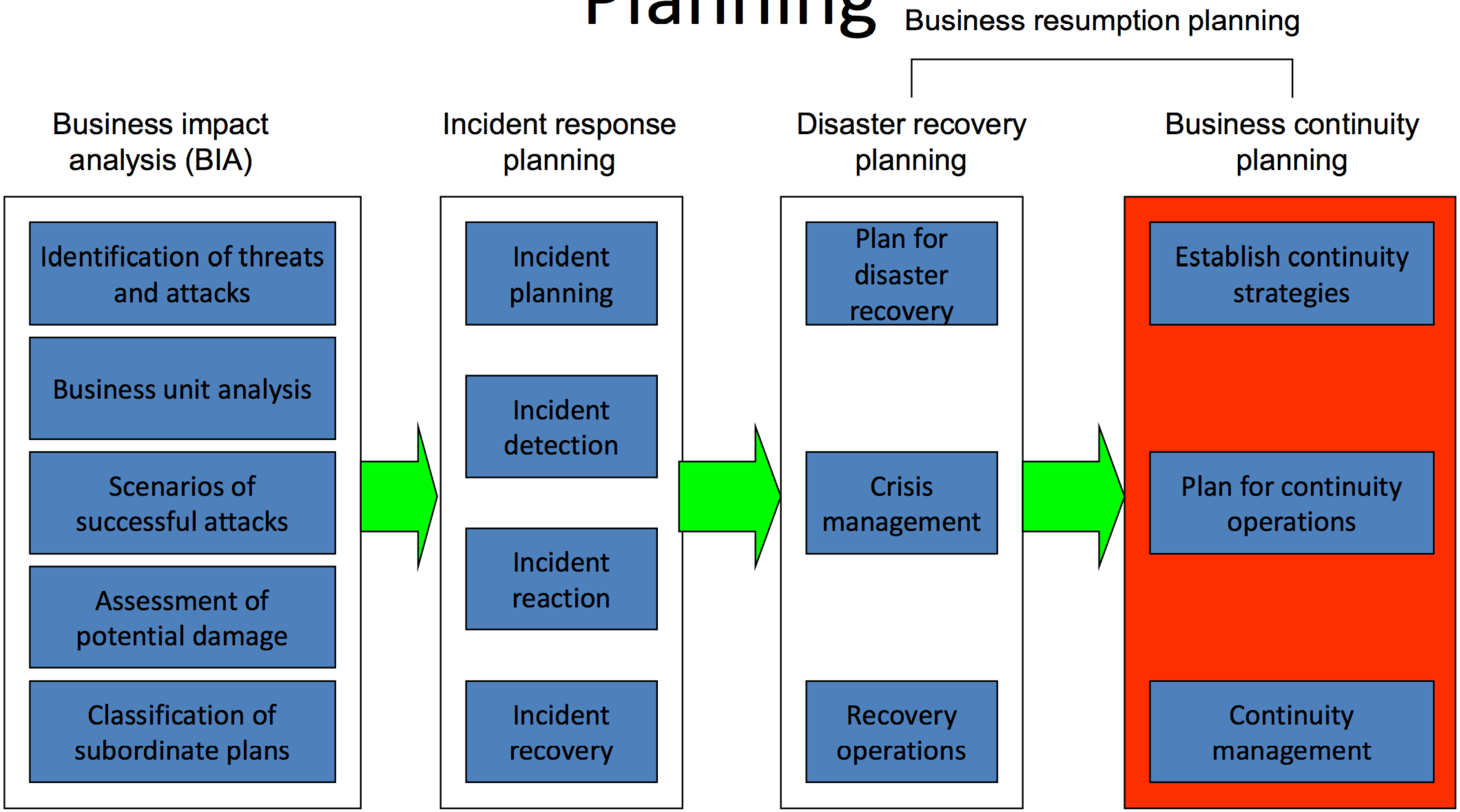
- NIST SP 800-34 is a good resource for contingency planning focusing on IT systems

- A "Contingency plan template" is available online at NIST's Computer Security Resource Center (CSRC)
  - Also see Appendix B in Whitman, Mattord and Green 2014
  - This is a combined DR/BC plan

BUSINESS RESUMPTION PLAN

- The DR and BC plan are closely related and many organizations combine them into a single planning document
  - May be called *Business Resumption Plan* or simply *Contingency Plan*
- A single team can develop the DR/BC plans, but execution of the plan requires separate teams
  - DR: Resuming operations at the normal operation facility
  - BC: Resuming operations at alternate site
- The DR/BC plans must also refer to the *Crisis Management Plan*

CP: Components of Contingency Planning



Business resumption planning

Business impact analysis (BIA)

- Identification of threats and attacks
- Business unit analysis
- Scenarios of successful attacks
- Assessment of potential damage
- Classification of subordinate plans

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 operations
- Continuity management

Because of lack of planning, over half of all the organizations that close their doors for more than a week, as a result of disruption, never open them again…

Whitman, Mattord and Green 2014, p. 439

BUSINESS CONTINUITY PLANNING: LESSONS LEARNED

- Plans must be kept current with emerging realities
  - Planning assumptions may change
  - Scenarios used in the planning may become outdated
- Training should never cease
- The real recovery will almost certain be different than the forecasted RTO and RPO
- Coordination relies on effective and accurate communications

FORMING THE BC TEAM

- Like DR team, includes representatives from every major organisational unit
- DR team members should be distinct from BC team members, as both may be activated at the same time
  - Senior management
  - Corporate support units (human resources, legal and accounting)
  - IT managers
  - A few IT technical staff
  - Infosec managers
  - A few infosec technicians

BC: SPECIAL DOCUMENTATION AND EQUIPMENT

- Each member of the BC team should have multiple copies of the DR and BC plans in their homes vehicles and offices

- Hardware:
  - Depends on the type and degree of coverage provided by the BC alternate site strategy
  - Ideally, only laptops, software media, licenses and backups of data
  - BC site provider usually provisions network equipment
  - Likewise for utilities

- Contact information require special attention (the phone numbers for important services may differ in the new site)

BC PLANNING: CONTINUITY PLAN DEVELOPMENT

- BC plan includes:
  - Detailed guidance and procedures for moving into alternate site
  - BC team leader is usually a general manager from operations or productions division
  - Subordinate BC plans
    - *Extent of BC plan activation depends on extent of damage*

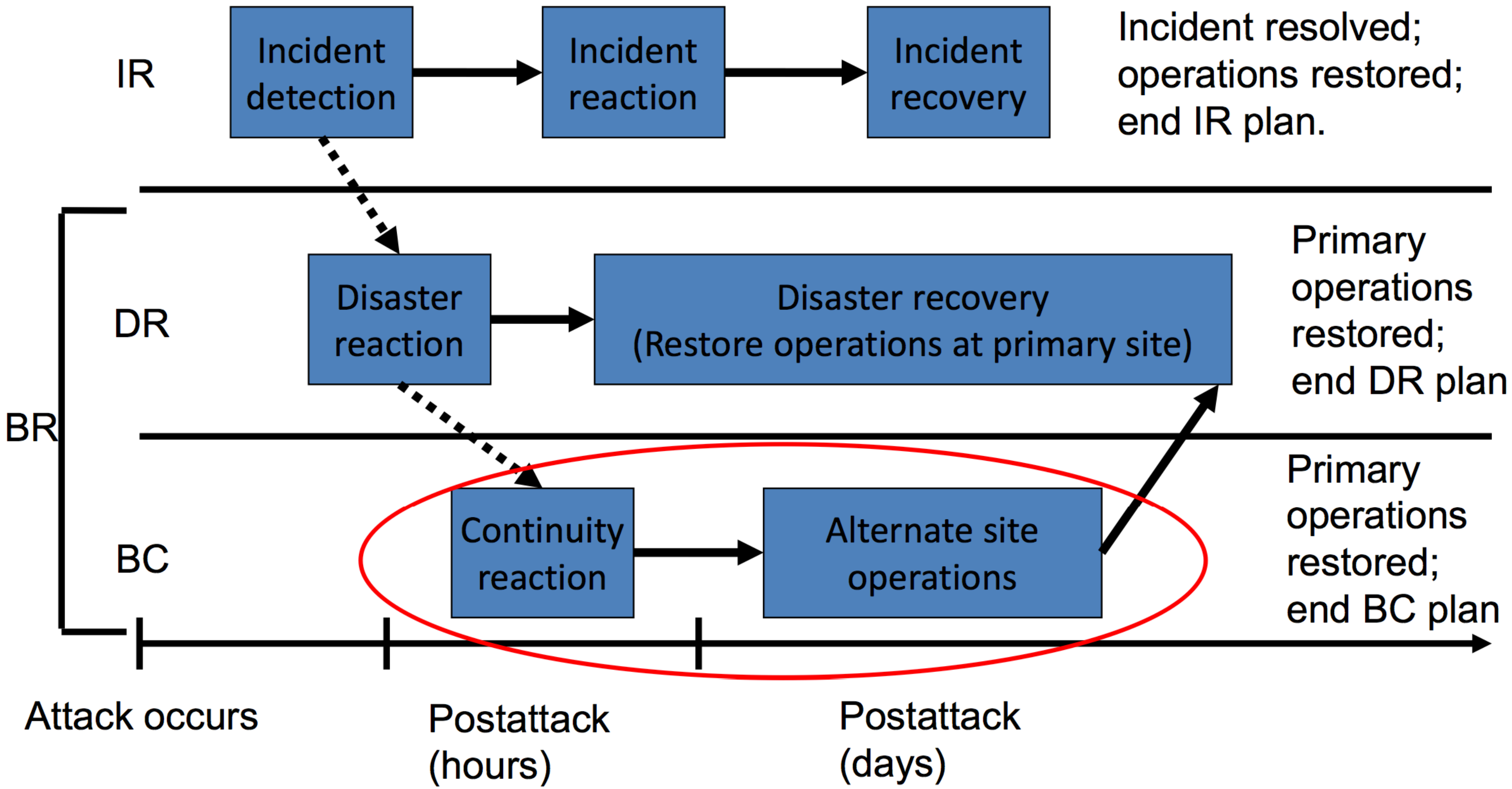
BC PLANNING: RELOCATION TO ALTERNATE SITE

- Identification of advance party, departure point and triggers
- Notification of service providers
- Notification of BC team to move to BC site
- Acquisition of supplies, materials and equipment
- Notification of employees to relocate to BC site
- Organization of incoming employees

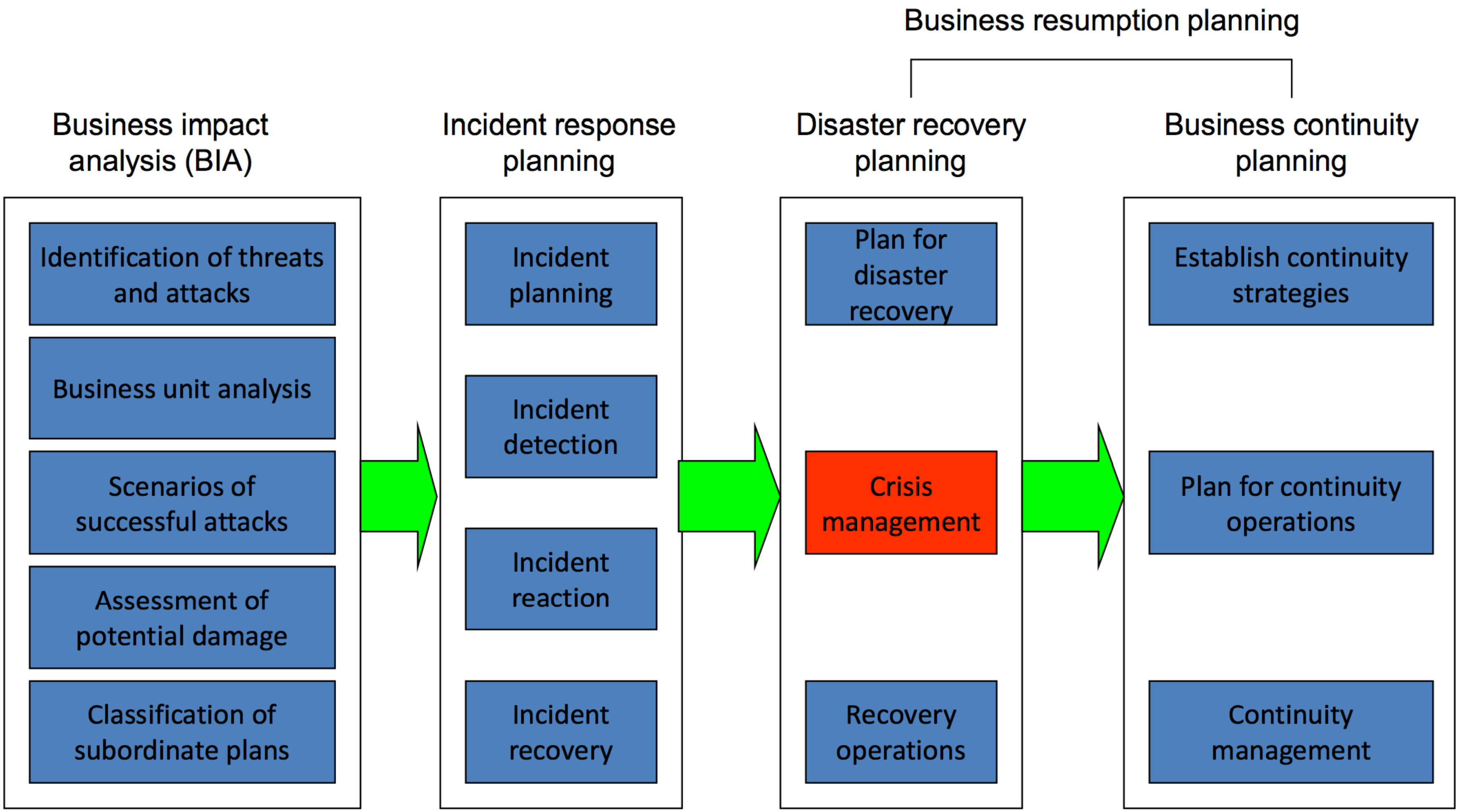
BC PLANNING: RETURN TO PRIMARY SITE

- Scheduling of employee move
- Vanguard clearing responsibilities
  - Disconnecting services
  - Breakdown of equipment
  - Packing and placing in storage or transporting to primary
  - Transfer of building to BC service provider and clearing

CP: Timeline for Contingency Plan Execution


IR
Incident detection
Incident reaction
Incident recovery
Incident resolved; operations restored; end IR plan.
BR
DR
Disaster reaction
Disaster recovery (Restore operations at primary site)
Primary operations restored; end DR plan
BC
Continuity reaction
Alternate site operations
Primary operations restored; end BC plan
Attack occurs
Postattack (hours)
Postattack (days)

Whitman and Mattord 2007, p. 27



Business resumption planning

Business impact analysis (BIA)

- Identification of threats and attacks
- Business unit analysis
- Scenarios of successful attacks
- Assessment of potential damage
- Classification of subordinate plans

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 operations
- Continuity management

Whitman and Mattord 2007, p. 27

NEXT LECTURE

The topic of the next lecture on the 12th of May will be:

Crisis Management and Human Factors

Recommended reading to prepare for the next lecture:

- Chapter 12 in Whitman, Mattord and Green