Business Continuity Planning & Disaster Recover

Introduction

- All organizations from all sectors (public, private and not-for-profit) face the possibility of disruptive events
  - These have impacts ranging from mere inconvenience and short-lived disruption of normal operations to the very destruction of the organization

BCP & DRP

- How to preserve critical business functions in the face of a disaster.

The BCP domain addresses:

- Continuation of critical business processes when a disaster destroys data processing capabilities
- Preparation, testing and maintenance of specific actions to recover normal processing (the BCP)

BCP - Not just an IT issue!

OUR COMPUTERS ARE DOWN, SO WE HAVE TO DO EVERYTHING MANUALLY...
[illegible] King Features Syndicate, Inc
6-25
Piccolo

Disasters – natural, man-made

- Fire, flood, hurricane, tornado, earthquake, volcanoes
- Plane crashes, vandalism, terrorism, riots, sabotage, loss of personnel, etc.
- Anything that diminishes or destroys normal data processing capabilities

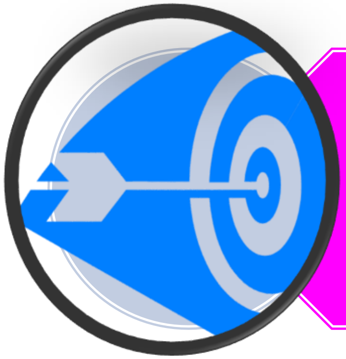
Disasters are defined in terms of the business

- If it harms critical business processes, it may be a disaster
- Time-based definition – how long can the business stand the pain?
- Probability of occurrence

Broad BCP objectives - CIA

Availability- Main Focus

Confidentiality – still important



Integrity – still important

BCP objective

- Create, document, test, and update a plan that will:
  - Allow timely recovery of critical business operations
  - Minimize loss
  - Meet legal and regulatory requirements
    - If the current business practice must meet such requirements then the BCP must preserve that compliance

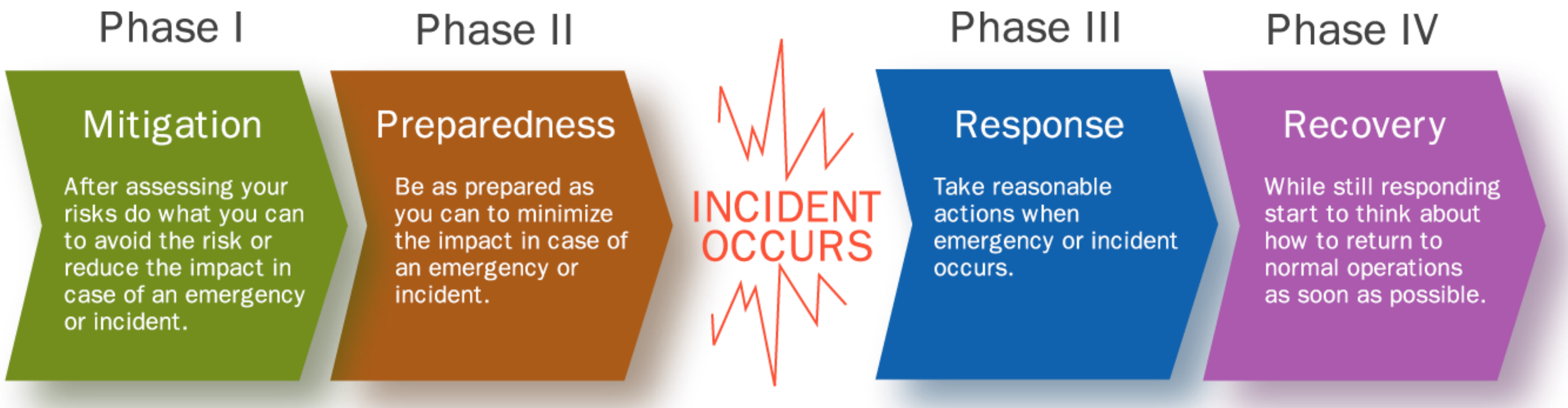
Scope of BCP

- Used to be just the data center
- Now includes:
  - Distributed operations
  - Personnel, networks, power
  - All aspects of the IT environment

Creating a BCP

- Is an on-going process, not a project with a beginning and an end
  - Creating, testing, maintaining, and updating
  - “Critical” business functions may evolve
- The BCP team must include both business and IT personnel
- Requires the support of senior management

Phases of Continuity Planning



Phase I

Mitigation

After assessing your risks do what you can to avoid the risk or reduce the impact in case of an emergency or incident.

Phase II

Preparedness

Be as prepared as you can to minimize the impact in case of an emergency or incident.

INCIDENT OCCURS

Phase III

Response

Take reasonable actions when emergency or incident occurs.

Phase IV

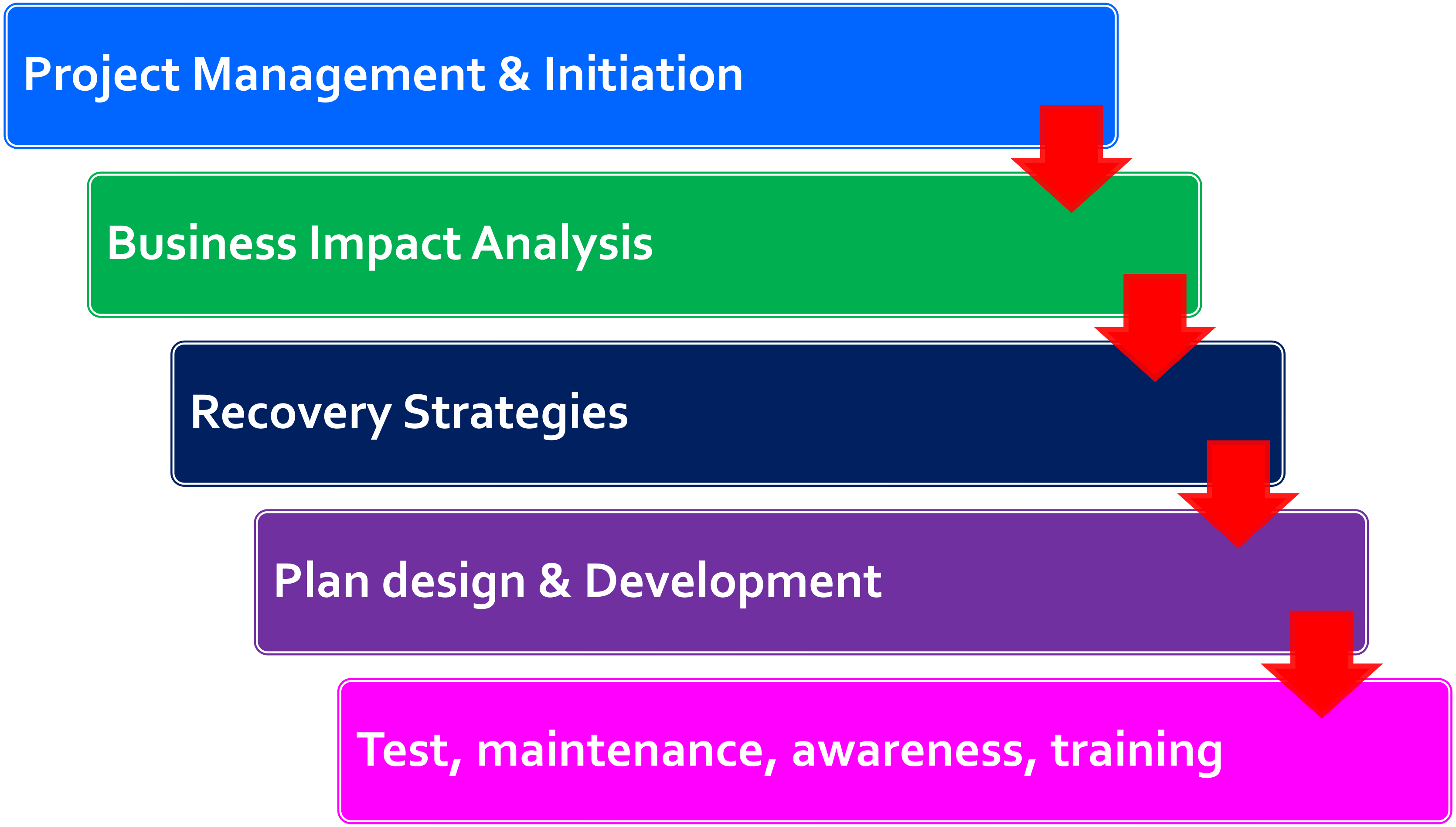
Recovery

While still responding start to think about how to return to normal operations as soon as possible.

Mitigation & Preparedness Occur Before an Incident

Response and Recovery Occur During & After an Emergency

The five BCP phases



Project Management & Initiation

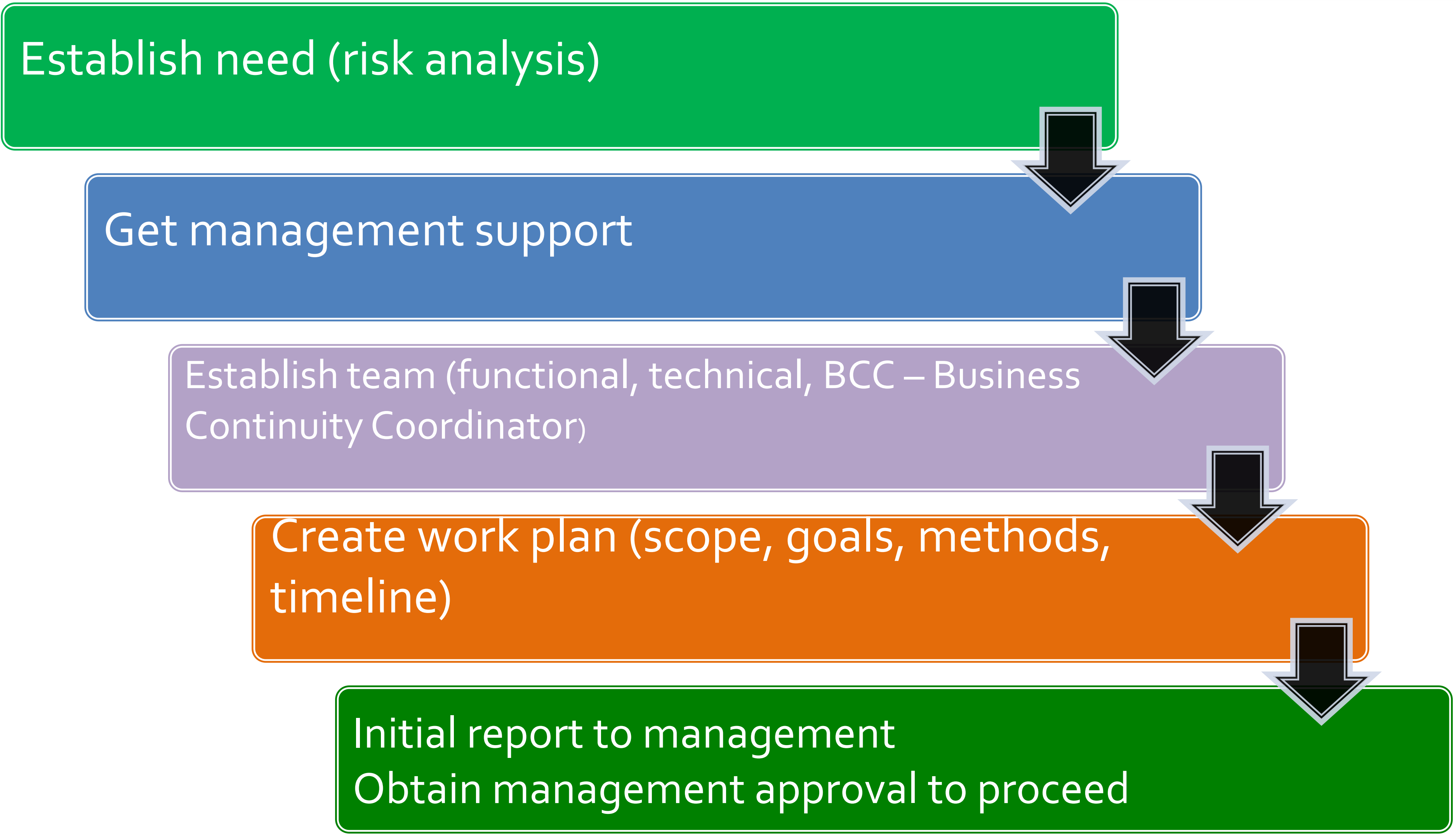
Business Impact Analysis

Recovery Strategies

Plan design & Development

Test, maintenance, awareness, training

I - Project management & initiation



Establish need (risk analysis)

Get management support

Establish team (functional, technical, BCC – Business Continuity Coordinator)

Create work plan (scope, goals, methods, timeline)

Initial report to management
Obtain management approval to proceed

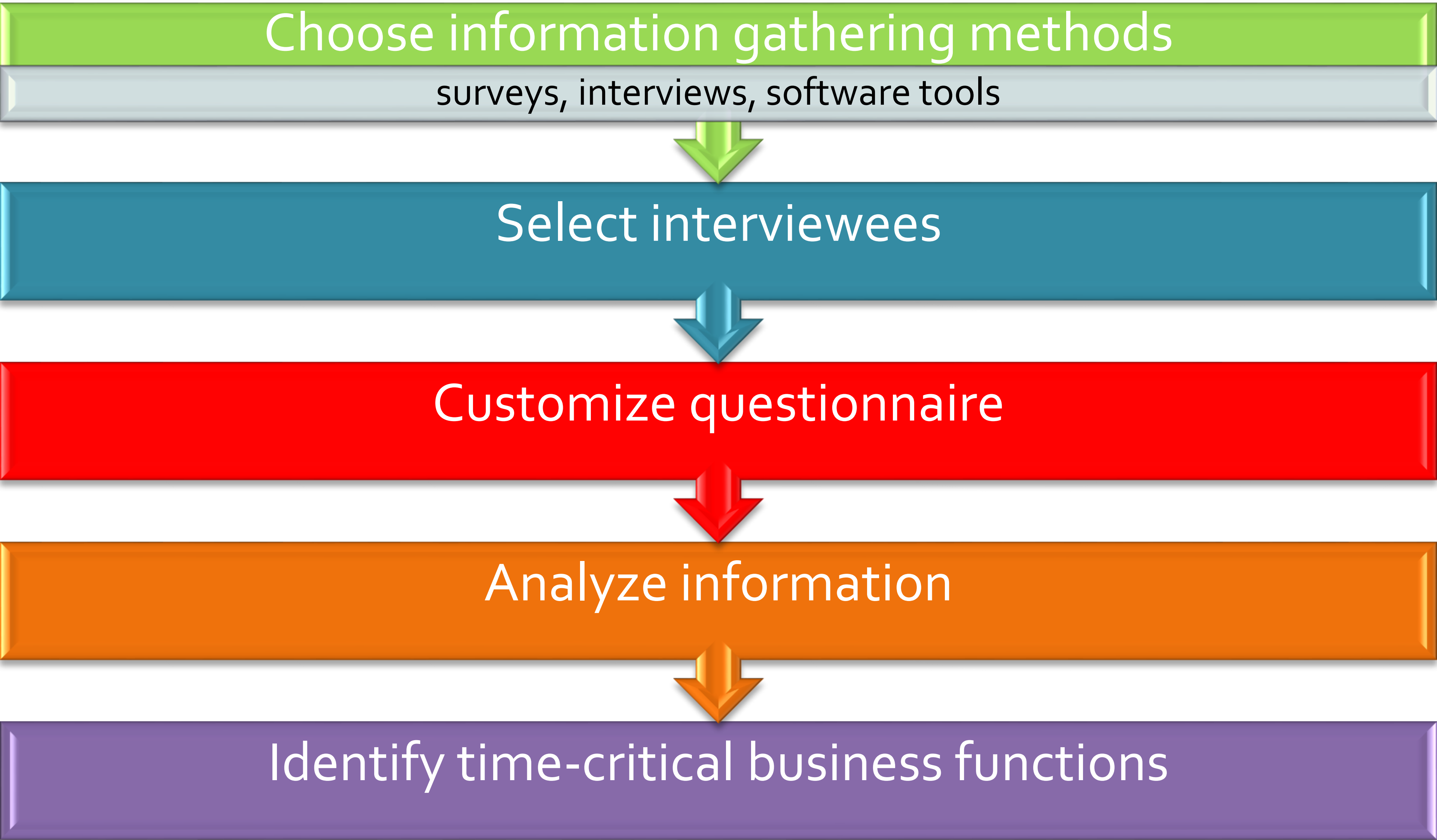
II - Business Impact Analysis (BIA)

- Goal: Obtain formal agreement with senior management on the MTD for each time-critical business resource
- MTD – maximum tolerable downtime, also known as MAO (Maximum Allowable Outage)

II - Business Impact Analysis (BIA)

- Quantifies loss due to business outage (financial, extra cost of recovery, embarrassment)
- Does not estimate the probability of kinds of incidents, only quantifies the consequences

II - BIA phases



Choose information gathering methods

surveys, interviews, software tools

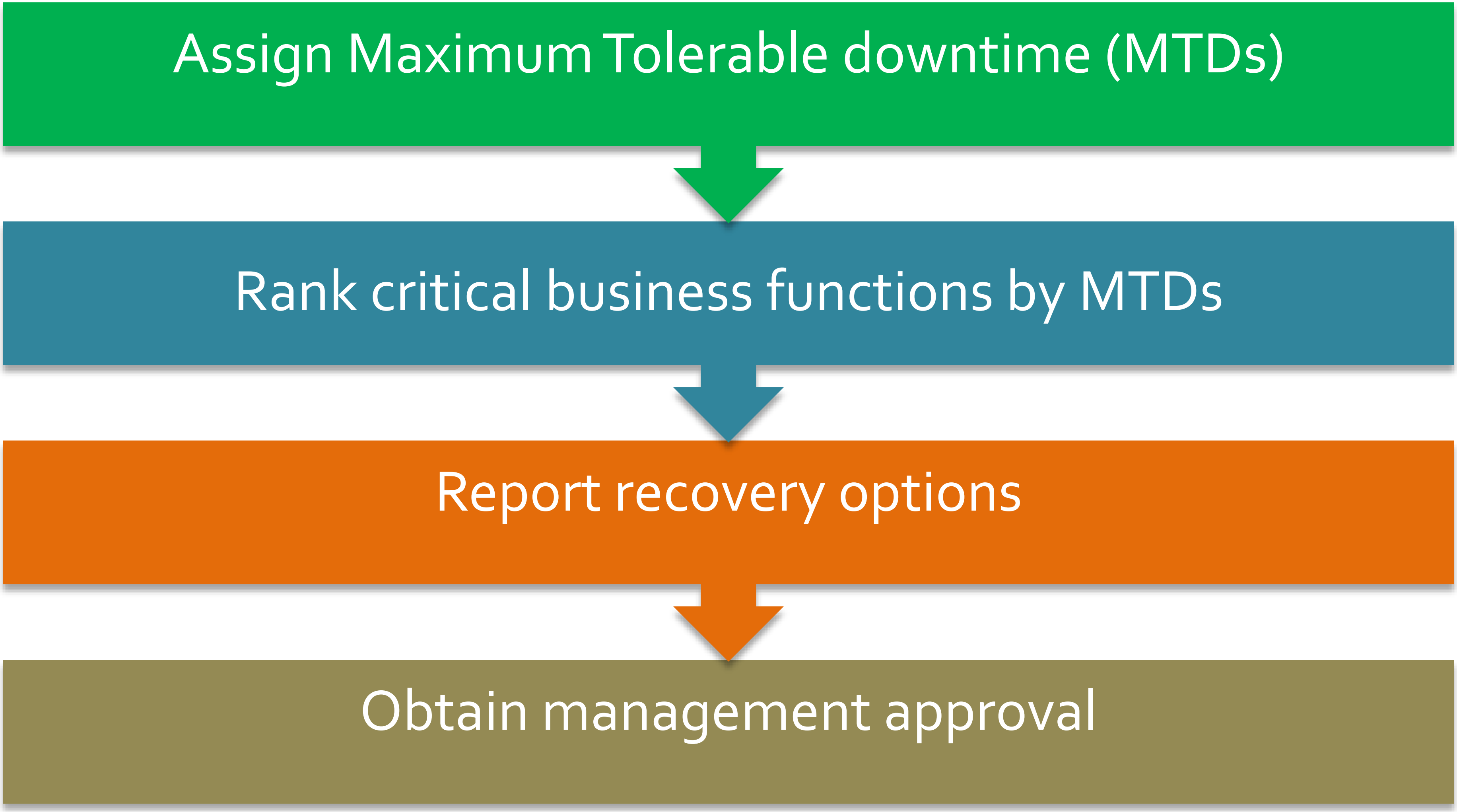
Select interviewees

Customize questionnaire

Analyze information

Identify time-critical business functions

II - BIA phases (continued)



Assign Maximum Tolerable downtime (MTDs)

Rank critical business functions by MTDs

Report recovery options

Obtain management approval

III – Recovery strategies

- Recovery strategies are based on MTDs
- Predefined
  - We don't have to make it up as we go along. We have documented, tested plan in place
- Management-approved
  - Means we will get the resources to implement BCP

III – Recovery strategies

- Different technical strategies
- Different costs and benefits
- How to choose?
- Careful cost-benefit analysis
- Driven by business requirements
    - Means going back to BIA, which identified critical business processes and ranked them in terms of the MTD/MAO

III – Recovery strategies

- Strategies should address recovery of:
  - Business operations
  - Facilities & supplies
  - Users (workers and end-users)
  - Network, data center (technical)
  - Data (off-site backups of data and applications)

III – Recovery strategies

- Technical recovery strategies - scope
  - Data center
  - Networks
  - Telecommunications

III – Recovery strategies

- Technical recovery strategies – methods
  - Subscription service sites
  - Mutual aid agreements
  - Redundant data centers
  - Service bureaus

III – Recovery strategies

- Technical recovery strategies – subscription service sites
  - Hot – fully equipped
  - Warm – missing key components
  - Cold – empty data center
  - Mirror – full redundancy
  - Mobile – trailer full of computers

III – Recovery strategies

- Technical recovery strategies – mutual aid agreements
  - I'll help you if you'll help me!
  - Inexpensive
  - Usually practically challenging

III – Recovery strategies

- Technical recovery strategies – redundant processing centers
  - Expensive
  - Maybe not enough spare capacity for critical operations

III – Recovery strategies

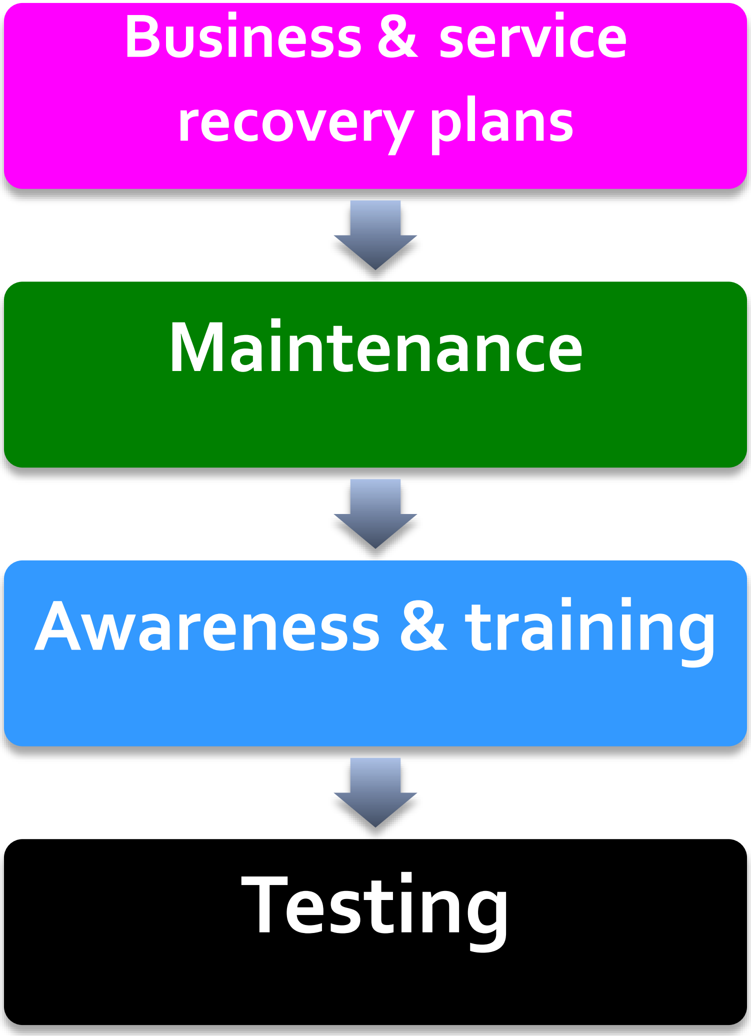
- Technical recovery strategies –service bureaus
  - Many clients share facilities
  - Almost as expensive as a hot site
  - Need negotiate agreements with other clients
    - If a client has to transfer operations to the service bureau as part of a DR, the other clients may take a hit in diminished processing capacity

III – Recovery strategies

- Technical recovery strategies –data
  - Backups of data and applications
  - Off-site vs. on-site storage of media
  - How fast can data be recovered?
  - How much data can you lose?
  - Security of off-site backup media

IV – BCP development / implementation

Detailed plan for recovery



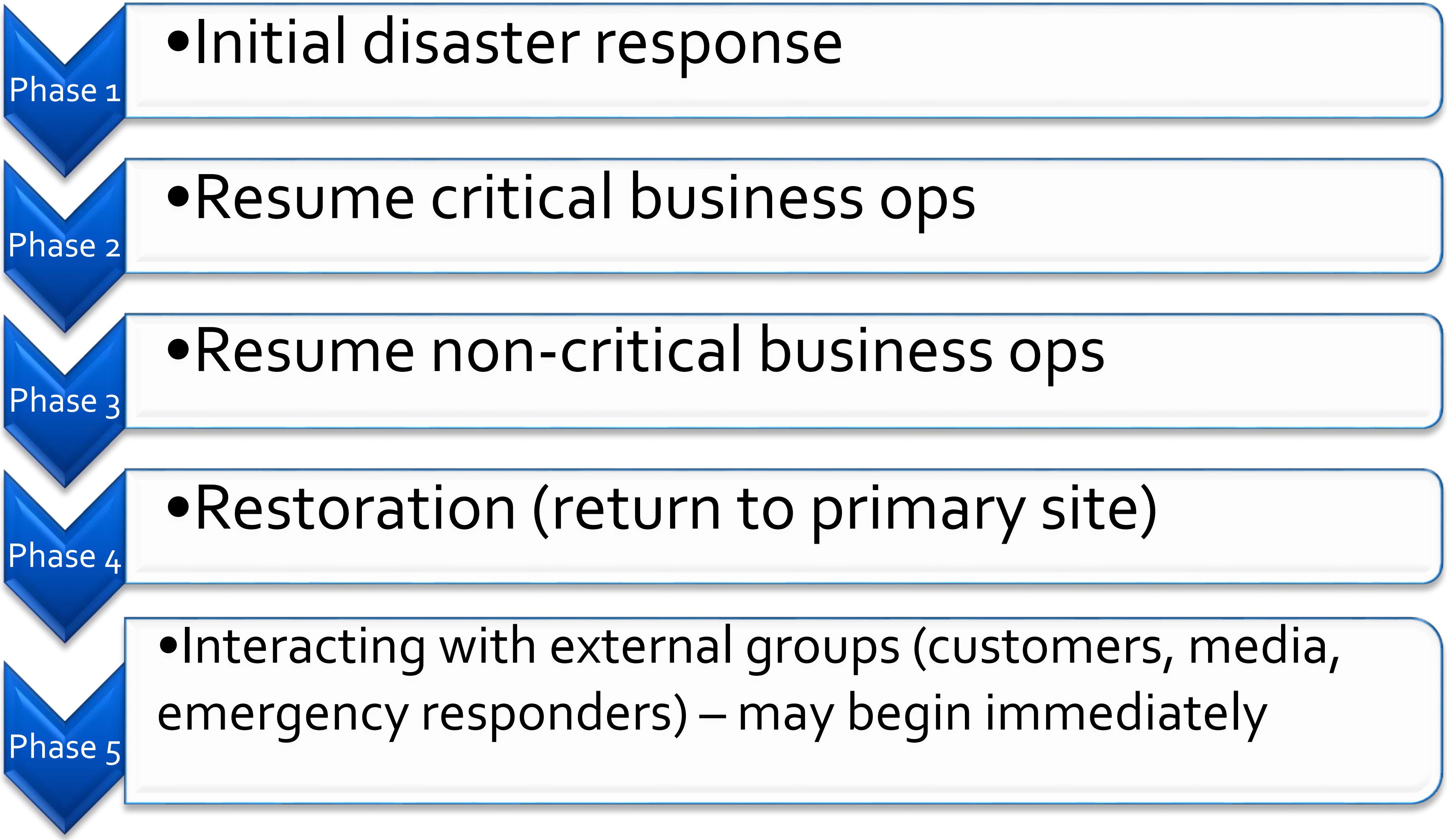
Business & service recovery plans

Maintenance

Awareness & training

Testing

IV – BCP development / implementation
Sample plan phases



Phase 1

- Initial disaster response

Phase 2

- Resume critical business ops

Phase 3

- Resume non-critical business ops

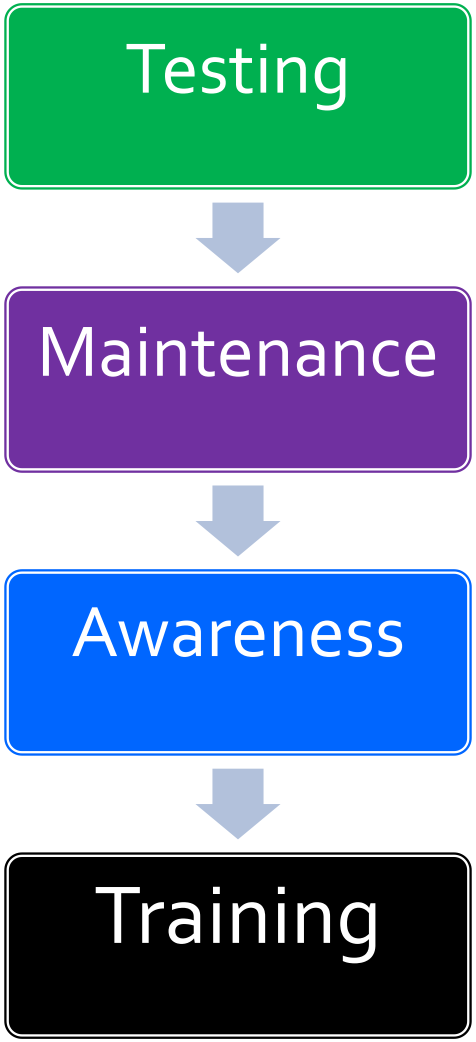
Phase 4

- Restoration (return to primary site)

Phase 5

- Interacting with external groups (customers, media, emergency responders) – may begin immediately

V – BCP final phase



V – BCP final phase - testing

- Until it's tested, you don't have a plan
- Kinds of testing
  - Structured walk-through – step by step review of BCP by functional reps
  - Checklist – given to business units to review
  - Simulation – role play
  - Parallel – DR site is put into full operation & results compared to the primary
  - Full interruption – full-scale test of BCP by planned fail-over to secondary site and fail-back to the primary

V – BCP final phase - maintenance

- Fix problems found in testing
- Implement change management
- Audit and address audit findings
- Annual review of plan
- Build plan into organization
- Continually maintain, update and improve the plan

V – BCP final phase - training

- BCP team is probably the DR team
- BCP training must be on-going
- BCP training needs to be part of the standard on-boarding and part of the corporate culture