Disaster Recovery



Kevin Henry
CISM CISSP CCSP

kevin@kmhenrymanagement.com

Outcomes of the Elements of a BCMS

Incident Response Planning

Life safety

Containment

Documentation

Return to Normal

Business Continuity Planning

BIA

CBFs

RTO

RPO

Recovery requirements

Disaster Recovery Planning

Relocation of IT and other services to an alternate location

Recovery Sites

Site Selection



RTO drives site selection

Faster recovery = higher costs

Systems recovery sequence based on criticality to the business

A manager may have employees and systems at different sites based on the process criticality

Selection of a Contingency Site

Cost	**Availability – meet RTO**	**Proximity – same threat**
Security	**Logistics - employees**	**Support**

Writing the Plan(s)



Writing the Response Plan

Written by the entire BCP team

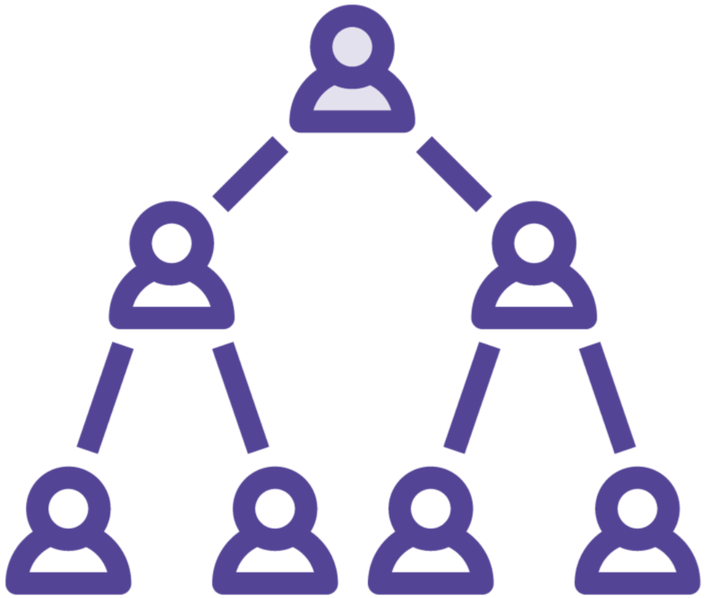
Action orientated

Plan written to address the most resource intensive situation (worst case scenario)

- **All lessor situations are included**

A crisis is a time of elevated risk
for an organization.
Many normal controls are missing.

Assign Teams



Roles and responsibilities

- Deputies
- Cross-training

Reporting relationships

Training and tools

Communication and Reporting

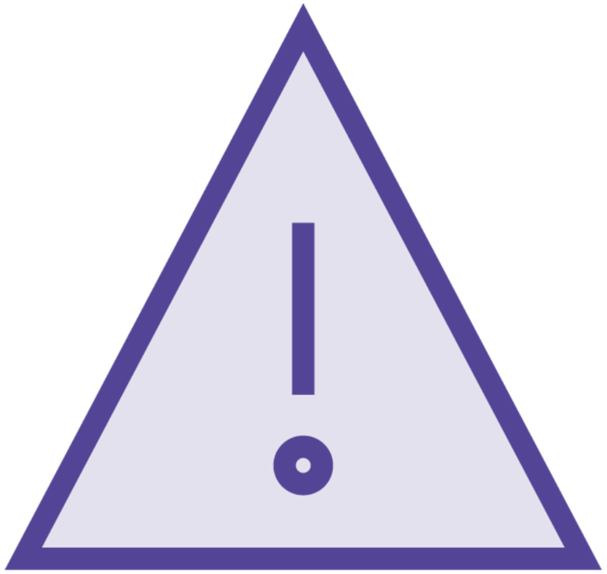


Stakeholders

- **Management**
- **Regulatory agencies**
- **Customers**
  - **Privacy breach**
- **Suppliers**
- **Shareholders**

Reporting

Report on status of crisis to management



Emergency Operations Center (EOC)



Milestones and progress

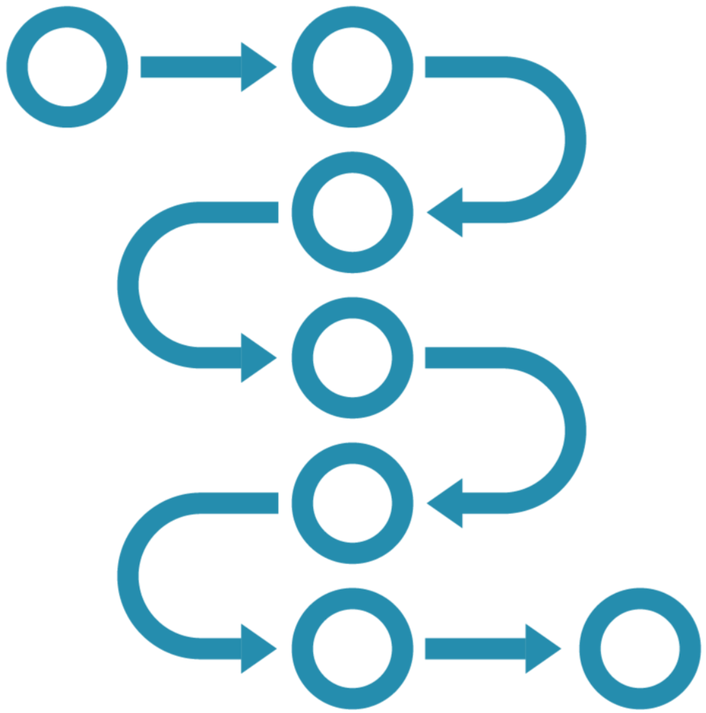
Restoration



The recovery of business functions prioritizes the most critical business processes first

Restoration to ‘normal’ starts with the least critical business functions first

Testing the Plan



Tests the plan

- **Find deficiencies**
- **Train staff**
  - **Develop skills**

Thorough tests

- **Realistic**

Start small – then increase in complexity

- **Apply lessons learned**

Summary



This module set out the requirements for disaster recovery planning – the most serious type of incident that requires the relocation of operations