Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts for CC℠

Incident Response



Kevin Henry
CISM CISSP CCSP

kevin@kmhenrymanagement.com

CC℠ Certification Examination

Domains	Weights
1. Security Principles	26%
2. Business Continuity (BC), Disaster Recovery (DR), & Incident Response	10%
3. Access Control Concepts	22%
4. Network Security	24%
5. Security Operations	18%

Exam Topics

Incident Response

Business Continuity

Disaster Recovery

Elements of a BCMS



Incident Response

Outcomes of the Elements of a BCMS

Incident Response Planning

Life safety

Containment

Documentation

Return to Normal

Business Continuity Planning

BIA

CBFs

RTO

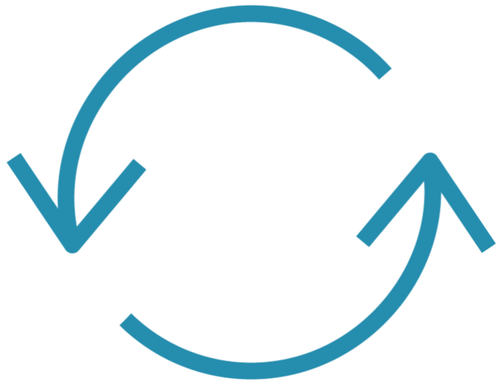
RPO

Recovery requirements

Disaster Recovery Planning

Relocation of IT and other services to an alternate location

Events Versus Incidents



Events – any measurable occurrence



Incidents – an adverse event with the potential to affect business mission

Business Resilience:
The ability to continue operations even during adverse circumstances

Response Planning



Historical events



Current threats

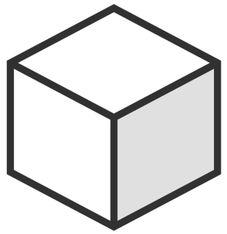


Areas of change

Incident Management



Preparation



Containment



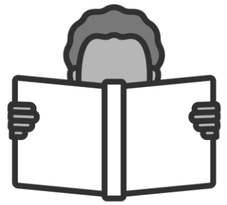
Prevention



Restoration



Detection



Lessons learned

Preparation

Policy

Team members

Documentation

Authority

Procedures

Reporting

Prevention



Offense drives defense

Monitor systems, networks, applications, users

Test controls

Awareness

Key Points Review



The secret to incident management is preparation – manage the incident and don’t let the incident manage you!

Prevention is better that recovery – learn from past incidents

Detection

Detection



Tools and technology

- Behavior analysis
- Signatures
- Heuristics

Alarms

Notification process for employees, customers, suppliers outside agencies

- Audit

Incident Detection



Helpdesk

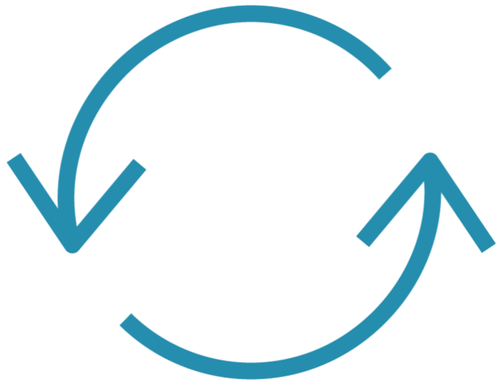
- Trouble tickets

Alerts

- Monitoring systems

Life Safety:
Always the first priority

Incident Classification

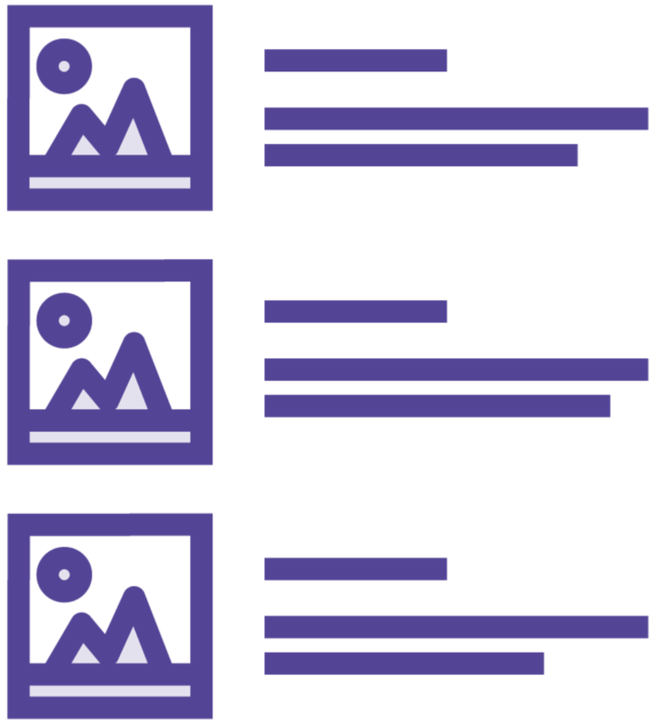


Noise – false positive



True positive

Incident Classification

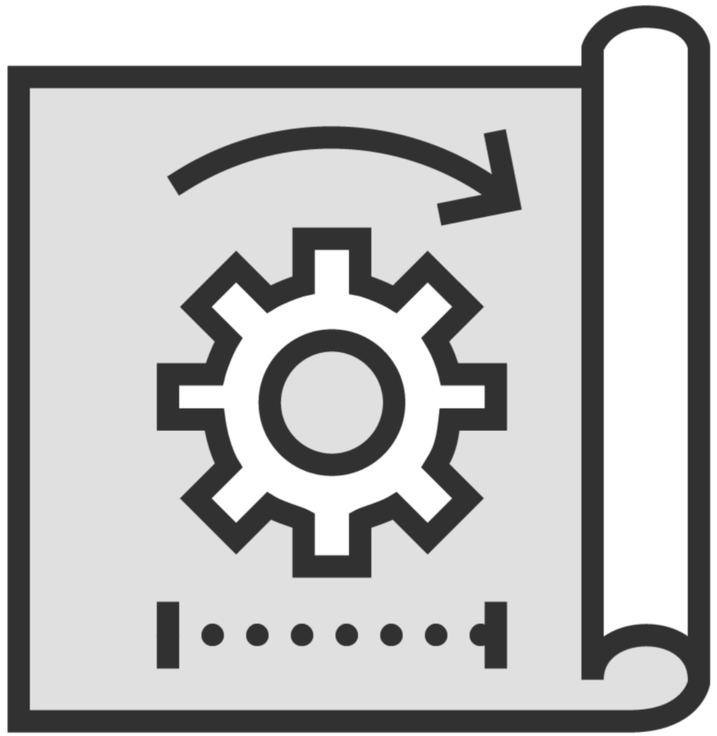


Minor

Serious

Catastrophic

Incident Classification



Internal

External

Intentional

Accidental

Activation of response teams

Containment Strategies



Isolation

- Fire doors
- Network connection
- Quarantine
  - Sandbox

Power down

Monitoring



Containment Considerations

Response depends on:

- Criticality
- Ability to spread
- Gathering of evidence

Key Points Review



Incident management starts with preparation and the ability to detect any incident

Then the ability to classify the incident and respond appropriately

Eradication



Eradication

Removal of damage

Re-build

- Backups
- Patches

Replacement of hardware

Restoration

Return to ‘normal’

Timelines
Prioritization of recovery

Prevent re-infection

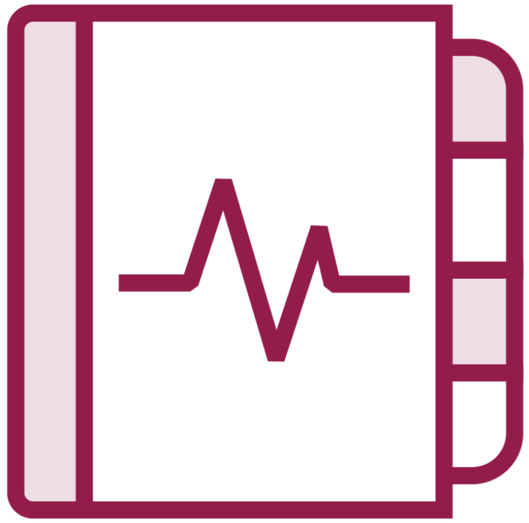
Documentation

Steps and procedures used in recovery

Retain to assist in future incidents

No need to ‘re-invent the wheel’ or repeat the same mistakes again

Reporting



Reporting on the conclusion of the incident

- What caused the incident
  - Multiple factors
- What was done to address and mitigate the incident
- Commendations for staff
- Lessons learned

Key Points Review



- **Incident response is a critical capability required for every business**
- **Senior management support is required**
- **Detailed plans and procedures are mandatory**
- **Teams must be properly trained and equipped**
- **The incident response plan must link to other plans such as BCP, DRP and Human Resources plans**

Post-incident Review Practices – Lessons Learned

Review



What went well?

What could be improved?

Who demonstrated competence and appropriate demeanor?

- Leadership

‘Hot wash’ versus ‘cold wash’

Lessons Learned

Improve:



Preparation

Training



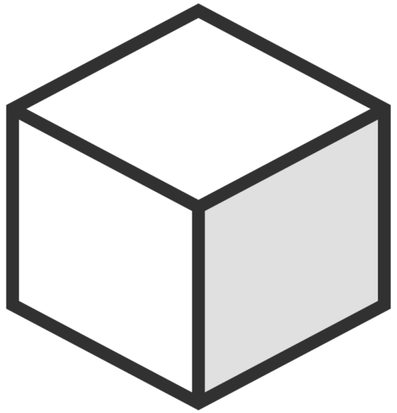
Prevention

Enhanced controls



Detection

Monitor the ‘right things’



Containment

Effective response

Awareness



Address lessons learned in awareness sessions

Improve staff training and consciousness of threats

Summary



Every incident contains key learning points that the organization can learn from

Seek to improve the incident response process and be better prepared for future incidents