

CDRE - Certified Disaster Recovery Engineer
Chapter 3 - BCP and DRP Design

WORKBOOK



BC Plan Design

Section 1

© Mile2 – All Rights Reserved



mile2
Cyber Security Certifications

BCP Design


BCP Limitations & Assumptions


- In any typical project management phase it is important to identify the “is” and “is not” of a project. You can ensure that there is no confusion or disagreement about what will, or will not be included within the scope of the BCP project. If for example, the BCP project will not be addressing multiple site disasters or loss of key personnel, document this as a limitation which will be addressed in subsequent BCP projects.

Here are some examples of assumptions:

- Staff are denied access to the office building for several days
- Addresses only critical business / revenue generating processes
- No more than one country will be affected concurrently by the same disaster
- Disaster occurs at the most vulnerable time for each business function
- Network link to DR site will remain intact

© Mile2 – All Rights Reserved






BCP Design

Business Recovery Organization and Responsibilities

- It is critical to define who the key people are and their responsibilities:
 - Business Continuity Coordinator (BCC)
 - Emergency preparedness & communications contacts
 - IT Disaster Recovery Coordinator
 - Employee assurance – helps employees families affected by disaster, so that employees can assist with business recovery
 - Operational team leaders – who manages the business during a disaster
 - Facility restoration and business resumption team leaders




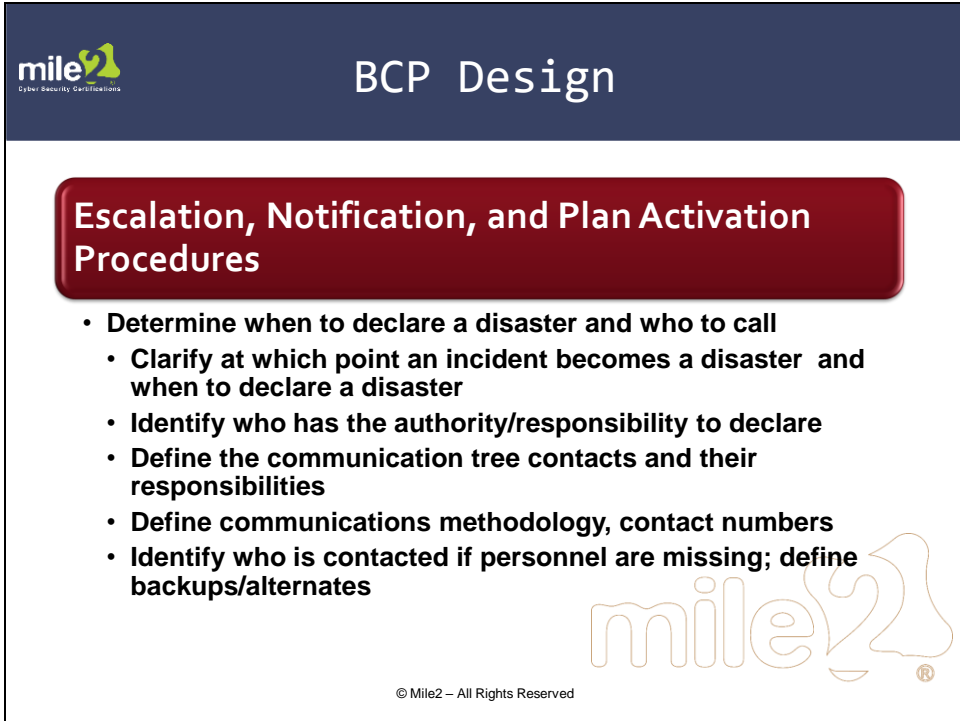
© Mile2 – All Rights Reserved

 **BCP Design**

Emergency Management Procedures

- **Define the steps to be taken in the event of a disaster or dangerous situation:**
 - **Emergency notification, alerts, warnings, announcements**
 - **Evacuation procedures**
 - **Rendezvous locations, local and remote, recovery site**
 - **Containment, remediation steps in cases of incident or emergency**
 - **Emergency & public safety & security services**


© Mile2 – All Rights Reserved



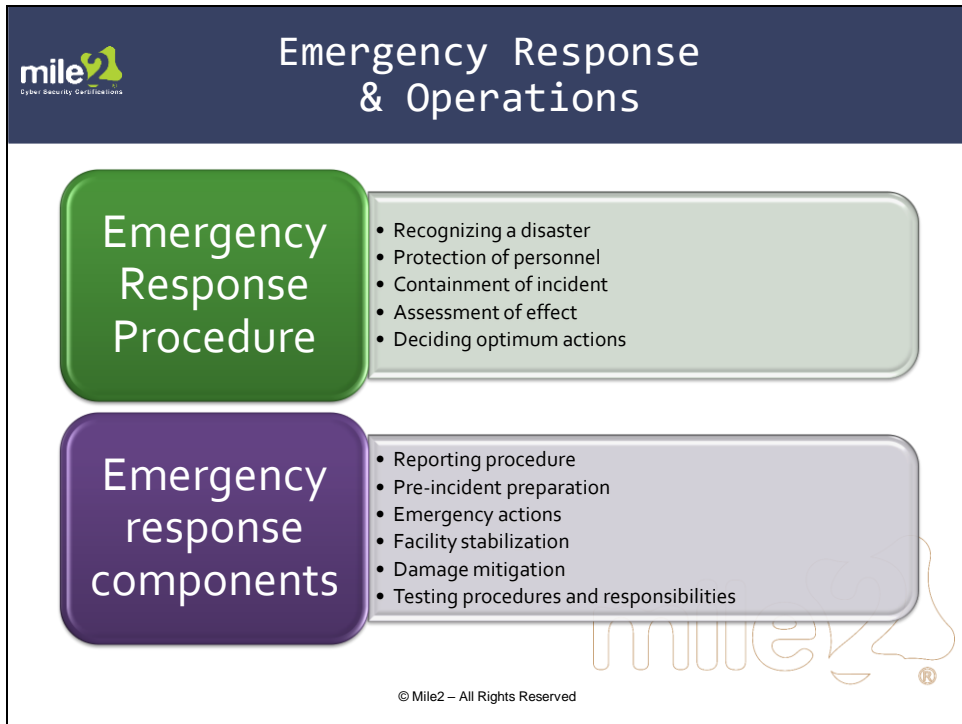
mile²
Cyber Security Certifications

BCP Design

Escalation, Notification, and Plan Activation Procedures

- **Determine when to declare a disaster and who to call**
 - **Clarify at which point an incident becomes a disaster and when to declare a disaster**
 - **Identify who has the authority/responsibility to declare**
 - **Define the communication tree contacts and their responsibilities**
 - **Define communications methodology, contact numbers**
 - **Identify who is contacted if personnel are missing; define backups/alternates**

mile²
© Mile2 – All Rights Reserved



The slide features a dark blue header with the Mile2 logo (a stylized '2' with a green and yellow dot) and the text 'mile2 Cyber Security Certifications'. The main title 'Emergency Response & Operations' is centered in white. Below the title, there are two main sections. The first section, 'Emergency Response Procedure', is in a green rounded rectangle and lists: Recognizing a disaster, Protection of personnel, Containment of incident, Assessment of effect, and Deciding optimum actions. The second section, 'Emergency response components', is in a purple rounded rectangle and lists: Reporting procedure, Pre-incident preparation, Emergency actions, Facility stabilization, Damage mitigation, and Testing procedures and responsibilities. A faint 'mile2' watermark is visible in the bottom right of the slide content area. The copyright notice '© Mile2 – All Rights Reserved' is at the bottom center.

Emergency Response Procedure

- Recognizing a disaster
- Protection of personnel
- Containment of incident
- Assessment of effect
- Deciding optimum actions

Emergency response components

- Reporting procedure
- Pre-incident preparation
- Emergency actions
- Facility stabilization
- Damage mitigation
- Testing procedures and responsibilities

© Mile2 – All Rights Reserved

The slide features a dark blue header with the Mile2 logo (a stylized '2' with a green leaf) and the text 'mile2 Cyber Security Certifications'. The main title is 'Emergency Response Components'. Below this, four colored rounded rectangles serve as section headers: red for 'Reporting procedures from command center', purple for 'Pre-incident preparation', dark blue for 'Facility stabilization (secure and limit access)', and teal for 'Damage mitigation (preventive actions / limit)'. The 'Pre-incident preparation' section contains a bulleted list of seven items. A small registered trademark symbol is visible at the bottom right of the slide content area.

Reporting procedures from command center

- Escalation
- Notification
- Damage assessment team


Pre-incident preparation

- Prepare for anything
- Emergency actions
- Evacuation
- Medical care
- Damage assessment
- Hazardous materials response
- Fire fighting
- Family assistance

Facility stabilization (secure and limit access)

Damage mitigation (preventive actions / limit)

© Mile2 – All Rights Reserved

 **Develop ER Procedures**

Recognizing a Disaster	<ul style="list-style-type: none">• Interruption or disaster• Determine severity criteria to determine difference• Design escalation criteria
Protection of People	<ul style="list-style-type: none">• Provide for communication with staff, next of kin, and dependents• Understand implications of statutory regulations (inspections, authorization, re-occupancy)
Containment of Incident	<ul style="list-style-type: none">• Practice salvage and loss containment• Create options to supplement emergency services to limit business impact
Assessment of Effect	<ul style="list-style-type: none">• Analyze situation and assessment report• Estimate impact on business and organization• Predict likely media interest and formulate response through public relations or designated spokesman
Deciding Optimum Actions	<ul style="list-style-type: none">• Understand issues before decision on recovery options (RTO)• Understand roles of emergency personnel• Maintain security of stored, archived assets

© Mile2 – All Rights Reserved

The slide features a dark blue header with the 'mile2 Cyber Security Certifications' logo on the left and the title 'ER Sources for Assistance' on the right. Below the header is a vertical stack of eight rounded rectangular buttons, each containing a source of assistance. The buttons transition in color from dark blue at the top to light green at the bottom. A small registered trademark symbol (®) is visible at the bottom right corner of the slide frame.

- Government emergency groups
- Safety and health organizations
- Fire Marshall
- Red Cross (training)
- Local emergency management coordinator
- Department of Homeland Security
- FEMA – Federal Emergency Management Agency

mile2
Cyber Security Certifications

BCP Design

End User, Business Unit Recovery Plans

- Business process continuation – manual steps to follow during IT outage
- Customer contacts – inform customers, alter expectations
- Staffing plans – initiate reduced emergency staffing
- Operational changes at recovery site, staffing, workspace, process changes
- Operational changes – deliveries, mail service, utilities, maintenance, communications – plan for all the normal maintenance items you may need for an extended period of time
- Transportation to / from and housing at recovery site
- Compensation, employee assistance

© Mile2 – All Rights Reserved

Public Relations Plans

- **Predetermine messages to public, customers, media**
- **Do not wait for a crisis to figure out what to say**
- **Present message focusing on human cost, all steps are being taken to ensure the safety of employees and the community**
- **Present a presence of calm, control, confidence**
- **Secondary message ensuring services, data is safe and available or recoverable**
- **ETA for resumption of services, facility rebuilds, etc. can come in succeeding announcements**


© Mile2 – All Rights Reserved

mile2
Cyber Security Certifications

Site Recovery & Resumption

Create site recovery and resumption plans at alternate site

- **Pre-planning will reduce time spent at recovery center**
- **Coordinate with insurer, property management, public officials to understand requirements to quickly rebuild / restore facilities**
- **Negotiate with hardware vendors to determine availability of technology and infrastructure and quick-ship requirements**



© Mile2 – All Rights Reserved


mile2®

Restoration of Primary Site

Restoration of primary site

- Ensure health and safety of staff to return
- Ensure IT systems are installed and functional
- Facility requires certification and accreditation

© Mile2 – All Rights Reserved

 **Return to Primary Site**

Return to primary site

- Management will decide when to vacate recovery site and return to primary site, or a new primary site
- Backup all data
- When returning home, if possible, process the least critical work first at the primary site as a validation for readiness
- Plan to coordinate changes in deliveries, mail service, communications


© Mile2 – All Rights Reserved



Disaster Recovery Plan

Section 2

© Mile2 – All Rights Reserved

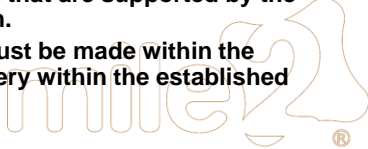
 **DR Plan Development**

Goal


- To provide information on the IT strategy and procedures for the recovery of the critical services and assets
- These plans and arrangements detail the ways and means to ensure critical services and products are delivered within the RTO by providing for the continued availability.
- The DR plans are based on the results of the BIA, the IT recovery requirements, and the IT recovery strategies. The plan will contact specific actions for each team, manager, or staff.

Scope

- Limited to the business units and services that are supported by the IT systems housed in the data center room.
- The decision to implement this BC Plan must be made within the timeframe after a disaster to ensure recovery within the established RTOs.



© Mile2 – All Rights Reserved



DR Plan Development


Objectives

- **Minimizing interruptions to the business's ability to provide the products and/or services**
- **Minimizing quantitative and qualitative loss of business**
- **Being able to resume critical operations within a specified time after a disaster.**
- **Executing the recovery strategy and steps to recovery critical services in the order of priority assigned to them**

Assumptions

- **The disaster will occur at the worst possible time, most or all of the business unit's critical data will be destroyed and access to the supporting IT systems will not be available.**
- **This document and all critical data are stored in a secure off-site location and not only survive the disaster, but are accessible immediately following the disaster**
- **Backup copies of system software, applications, and databases are stored in a controlled environment at an offsite location.**

© Mile2 - All Rights Reserved




DR Plan Development

IT Recovery Plan

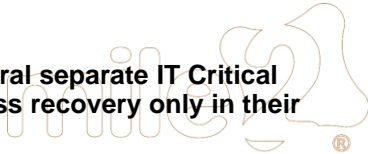
- IT is responsible for maintaining the operational and recovery process documentation for each system and application
- Each application process or technology has a restoration / recovery plan designed to meet RTO & RPO defined in the BCP
- DR plans "cookbook" can include:
 - Descriptions of backups, location, retrieval information
 - Descriptions of recovery site location, contact and access information, startup procedures
 - Software license keys, vendor account information, admin accounts and password retrieval instructions
 - Location of software installation media and documentation
 - Documented process to recover technologies (Oracle, Windows, SQL, Exchange, Network firewall, Phone systems, etc.)
 - Application diagrams listing which system and data components make up an application process
 - Application integration documentation, data flow diagrams, startup & verification instructions
 - Recovery order, step by step instructions to recover systems and applications in the appropriate order to meet business recovery time objectives

© Mile2 – All Rights Reserved

 **DR Plan Development**

IT Recovery Teams

- **For a small IT site, the IT Critical Support Function Team may be a single recovery team that addresses:**
 - LAN recovery
 - WAN recovery
 - IT Hardware Platform recovery
 - Network recovery
 - Software recovery (Data and Database)
 - Applications recovery
 - Communications recovery
- **For larger IT sites, there may be several separate IT Critical Support Functions Teams that address recovery only in their respective areas**



© Mile2 – All Rights Reserved

 **DR Plan Development**


As can be noted:

The **devil is in the **details**!**

There will be a vast amount of details depending on the size and complexity of the environment to be recovered. Accurate documentation and exact records management will be essential.



© Mile2 – All Rights Reserved

 **DR Plan Design**

Contents of a DR Plan

- Title of DR Team
- Plan Overview, Scope, Objectives, and Assumptions
- General Team Information
 - Names and contact information
 - Roles & Responsibilities
- List of Critical Business Units and Service IT requirements
 - IT hardware/software, data, IT standard operating procedures
- Recover to alternate site
 - Tasks to recover Critical Services at Alternate Site
 - Resumption of critical services
- Location of alternate site
- Restoration of primary site procedures
- Return to home site procedures


© Mile2 – All Rights Reserved

The slide features a dark blue header with the 'mile2 Cyber Security Certifications' logo on the left and the text 'End of Chapter 3' on the right. In the center, there is a prominent red button with rounded corners containing the text 'Moving Forward'. The bottom right corner contains a large, light-colored 'mile2' logo and a small copyright notice: '© Mile2 - All Rights Reserved'.

Questions

and

Answers

Review Questions:

1. Which is included in the Risk Analysis process?
 - A. Identify threats to critical elements
 - B. Identify vulnerabilities of critical elements
 - C. Identify & analyze existing controls
 - D. All of the above

2. Which is the most common cause of unplanned downtime?
 - A. Natural disasters – flood, hurricane, earthquake
 - B. Environment – power, A/C, etc.
 - C. People and processes – human error

3. Recovery priority of a business process is determined in the:
 - A. Risk Analysis
 - B. Business Impact Analysis
 - C. Technology Analysis
 - D. Gaps Analysis

4. Which is a hazard or danger, chance, or probability of loss or consequence?
 - A. Risk
 - B. Threat
 - C. Vulnerability

5. Which is a cause or indication of unwanted event that can cause loss?
 - A. Risk
 - B. Threat
 - C. Vulnerability

6. Which is an exposure to threat or unwanted event?
 - A. Risk
 - B. Threat
 - C. Vulnerability

Answer Key:

1. D
All of the options are included in the risk analysis process.
2. C
Human error is the most common cause of unplanned downtime.
3. B
Recovery priority of a business process is determined in the business impact analysis.
4. A
A risk is a hazard or danger, chance, or probability of loss or consequence.
5. B
A threat is a cause or indication of unwanted event that can cause loss.
6. C
A vulnerability is an exposure to threat or unwanted event.