

Business Continuity and Disaster Recovery Planning

Agenda

- Business Continuity Planning Concepts
- Business Continuity Planning Overview
 - Initial Planning
 - Risk Analysis
 - Business Impact Analysis (BIA)
 - BC Plan Design and Development
 - BC Plan Implementation
 - Maintaining and Exercising BC Plan
- Summary

Business Continuity Planning Concepts (1)

Disaster – a Definition

A sudden, unplanned calamitous event causing great damage or loss. In the business environment, any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time.

Source: Disaster Recovery Institute International (DRII),
USA

Business Continuity Planning Concepts (2)

What is a Business Continuity?

Business continuity management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

(Source: British Standards Institute PAS 56)

Business Continuity Planning Concepts (3)

What is a Disaster Recovery?

Recovery of the computing environment from an error or major site failure to an acceptable condition.

☛ Disaster Recovery is a subset of Business Continuity

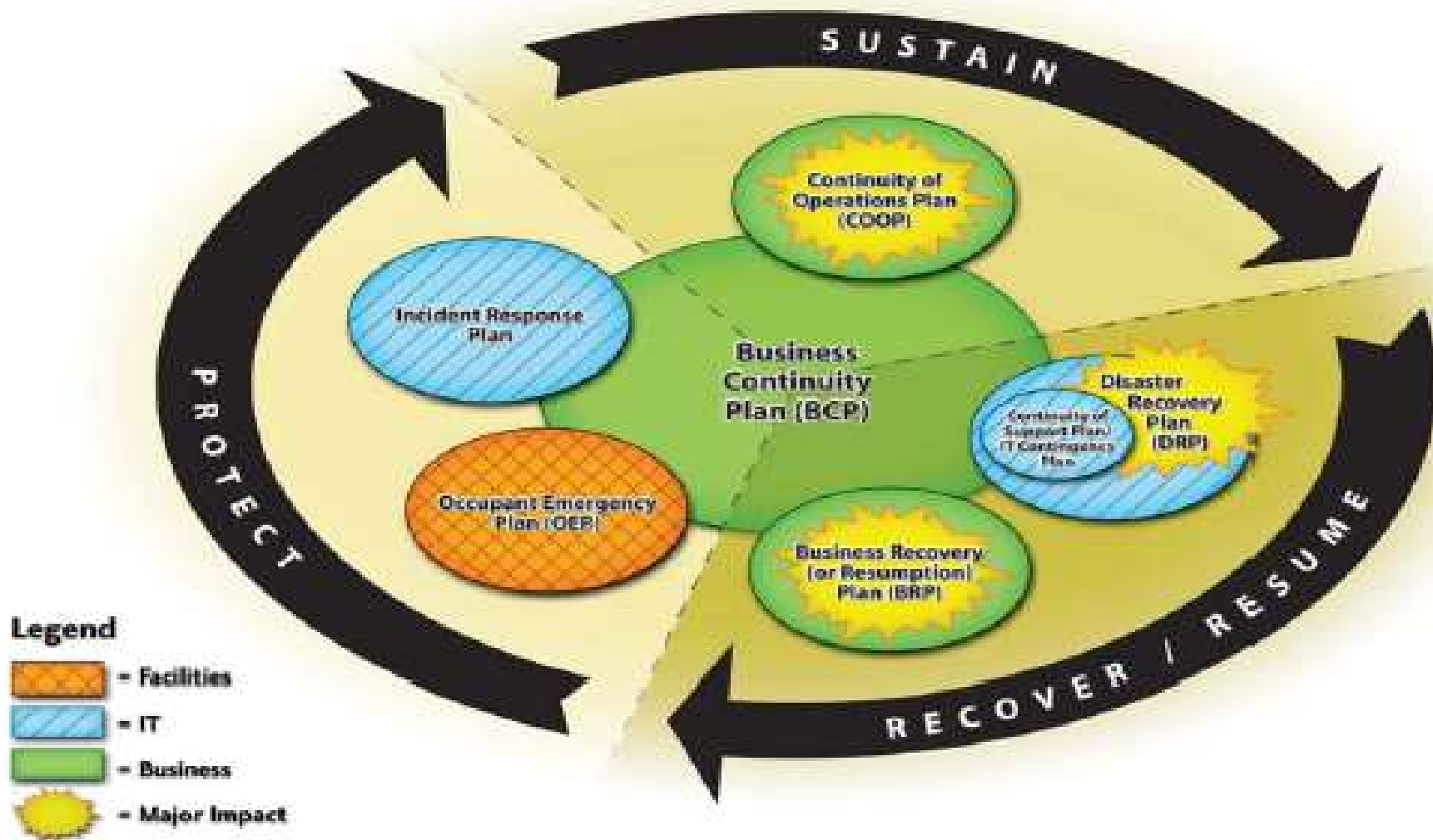
Business Continuity Planning Concepts (4)

Difference Between BCP & DRP

- Business continuity planning deals with the continuity of critical business processes
- With the BCP, the company could reduce the impact a disaster could have to the normal business operation
- The DRP covers the restoration of the critical information systems that support the business processes

Business Continuity Planning Concepts (5)

BCP Variants



Business Continuity Planning Concepts (6)

Why Have a BCP / DRP?

- Plan for the worst, hope for the best
- Preparation reduces poor performance
- A BCP is a business's last line of defence against risks that cannot be controlled or avoided by other risk management practices
- Maintain business operations – Or at least, restore operations quickly
- Effect on customers or stakeholders

Business Continuity Planning Concepts (7)

Why Have a BCP / DRP? (contd...)

- Regulatory Requirements
 - Sarbanes-Oxley Act
 - Basel II (outlined 7 high level BCP Principles)
 - Central Banks of India, Hong Kong, Singapore, Malaysia, Philippines, Japan, Australia

Business Continuity Planning Concepts (8)

- Laws of Business Continuity
 - i. Prevention is better than cure
 - ii. Deploy only as much high availability as you really need, but not less than you need
 - iii. Only a comprehensively tested system provides business continuity
 - iv. The process of business continuity planning is more important than the Plan itself

Business Continuity Planning Concepts (9)

Common BCP Fallacies

- It won't happen to us
- Our staff can handle the situation
- It costs too much

Business Continuity Planning Concepts (10)

Disaster Preparedness

- 38% of organisations in EMEA do not know how long it would take to recover from a fire disaster
 - Average recovery time of organisations that do know is **3.23 days**
 - Only **3%** said they could carry on with business as usual if a disaster happened

Source: VERITAS Disaster Recovery Research

Business Continuity Planning Concepts (11)

- Top 5 consequences of disasters:
 1. Decreased employee productivity (62%)
 2. Data loss (43%)
 3. Reduction in profits (40%)
 4. Damage to customer relationships (38%)
 5. Reduction in revenue (27%)

Source: VERITAS Disaster Recovery Research

Business Continuity Planning Overview

- Initial Planning
- Risk Analysis
- Business Impact Analysis (BIA)
- BC Plan Design and Development
- BC Plan Implementation
- Maintaining and Exercising BC Plan

Initial Planning

- Management buy-in
- Budgeting and Resources
 - Budget available
 - Staff available
 - Skills available
 - Time available
 - Infrastructure available

Risk Analysis (1)

Risk Analysis – a definition

The process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure, and evaluating the cost for such controls.

Source: Disaster Recovery Institute International (DRII), USA

Risk Analysis (2)

Objectives of Risk Analysis

- Identify threats to organization
- Estimate probabilities of those threats occurring
- Identify the risks to organizational assets if those threats occur
- Identify costs to organization to establish effective controls to reduce risks

Risk Analysis (3)

Risk Analysis Terminology

- Vulnerability
 - Weakness in a system, technology, design, or plan
- Threat
 - Event that causes a risk to become an actual loss to company assets
- Risk
 - Exposure to loss, injury, danger; potential for loss

Risk Analysis (4)

Typical Disaster Scenarios

- Natural disasters
 - Earthquakes
 - Tornadoes & wind storms
 - Floods
 - Volcanic eruptions
- Political disasters
 - Riot and civil disturbances
 - Terrorist attacks
- Man-made / Technological disasters
 - Fires
 - Explosions / Bombings
 - Sabotage
 - Utility failure
 - Burst pipes
 - Building collapse
 - Environmental contamination
 - Hacking

Risk Analysis (5)

Risk Analysis Techniques

- Qualitative
 - Relates cause and effect (threat and risk) while identifying vulnerability; descriptive
- Quantitative
 - Identifies cost of a particular effect, incident, or phenomenon; assigns monetary value
- A combination of both (semi-quantitative)

Business Impact Analysis (1)

Business Impact Analysis (BIA) Defined

The process of determining the impact on an organization should a potential loss identified by the risk analysis actually occur. The BIA should quantify, where possible, the loss impact from both a business interruption (number of days) and a financial standpoint.

Source: Disaster Recovery Institute International (DRII), USA

Business Impact Analysis (2)

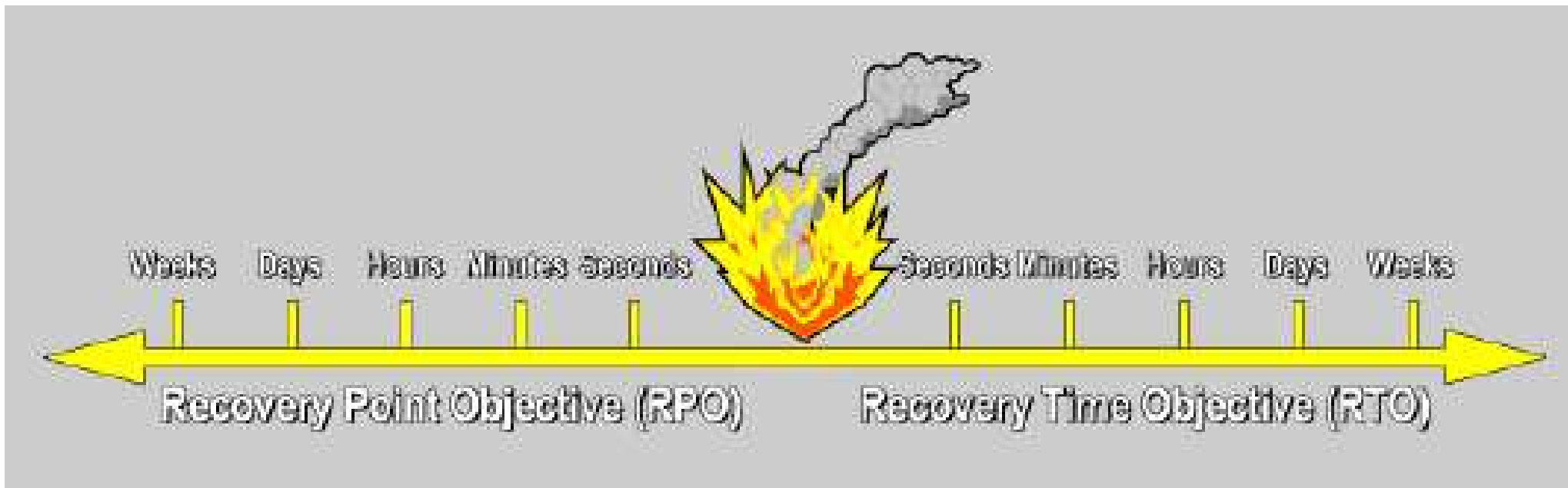
Objectives of Business Impact Analysis (BIA)

- Identify the business critical functions
- Assess impact of outage on these functions
- Determine the minimum resources needed during disasters
- Determine the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Identify the Vital Records needed

Business Impact Analysis (3)

RTO: The length of time a company can tolerate the absence of a particular function or information asset

RPO: How up-to-date does the data need to be? (has to do with data freshness)



Business Impact Analysis (4)

Steps in conducting BIA

- Determine the impact to the company of an outage on each department. Consider:
 - Revenue impact and Indirect costs
 - Reputation impact
 - Legal / regulatory impact
- Identify the **business processes** performed by the department and rate their level of importance as:
 - Must to Have (for Mission Critical processes)
 - Need to Have (Essential processes)
 - Good to Have (Desirable processes)

Business Impact Analysis (5)

Steps in conducting BIA (contd...)

- Further analyze the 'Must to Have' and 'Need to Have' processes:
 - to understand the workflow and day-to-day processing requirements,
 - develop appropriate recovery strategies, and
 - Identify the implementation requirements like:
 - Business recovery / alternate site requirements
 - Vital records requirements
 - Report Requirements

BC Plan Design & Development (1)

Steps in Design & Development of BC Plan

- Define BC Plan Scope, Levels of Continuity and Objectives
- Define Recovery Organization, Recovery Teams and their Roles and Responsibilities
- Define Escalation, Notification and Plan Activation Procedures
- Define Vital Records and Off-Site Storage Program

BC Plan Implementation (1)

Steps in Implementation of BC Plan

- Define Emergency Response Procedures (evacuation)
- Define Command, Control and Emergency Operations Center (Crisis Management) Procedures
- Define Detailed Resumption, Recovery and Restoration Procedures
- Enter into Contracts with Vendors
- Procure necessary Recovery Resources

Maintaining and Exercising BC Plan (1)

- Testing and Exercising
 - Four Types of Tests
 - ❖ Call Test
 - ❖ Tabletop or Walkthrough Test
 - ❖ Simulated Test
 - ❖ Actual Test
 - Training and Organisational Awareness Programs

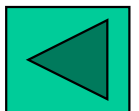
Maintaining and Exercising BC Plan (2)

- Maintenance and Updating
 - Schedules and Budgets for Update and Maintenance
 - Review Criteria
 - Program Status and Reporting
 - Business Continuity Audits

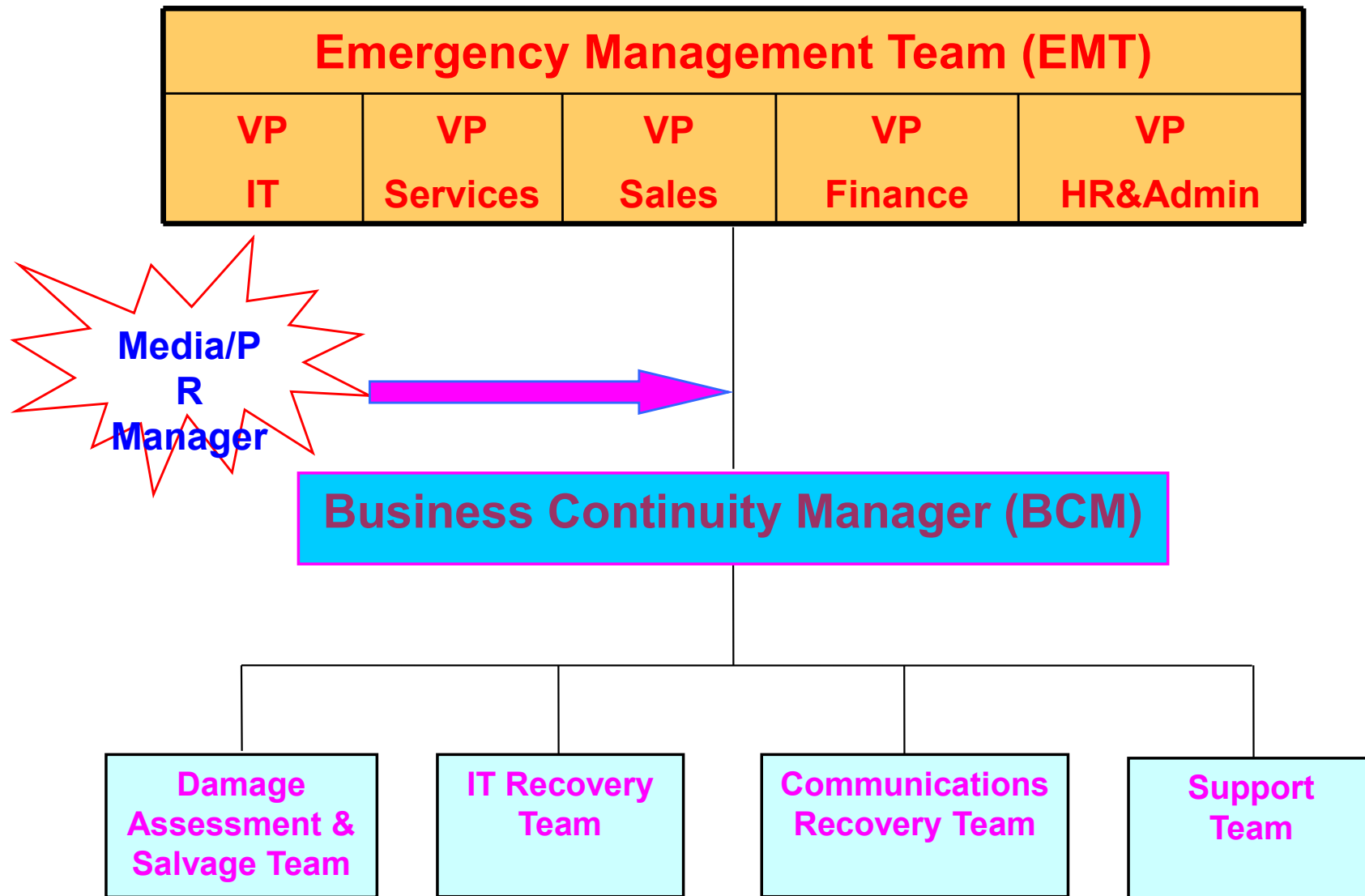
Thank you!

Disaster Recovery Strategies

- Backup Methods
- Process Manually
- Provide alternative source of products
- Alternate Sites
 - Cold Sites
 - Warm Sites
 - Hot sites
 - Mirrored sites
- Reciprocal Agreements
- Equipment Replacement (SLAs)
- Build Resilience
- Transfer Risk (via insurance / contracts)



Recovery Organization Structure



Four Levels of Continuity

- i. Platform-level Continuity
- ii. Data-level Continuity
- iii. Application-level Continuity
- iv. Site-level Continuity

