



Business Continuity Management

The Basics

October 5, 2004

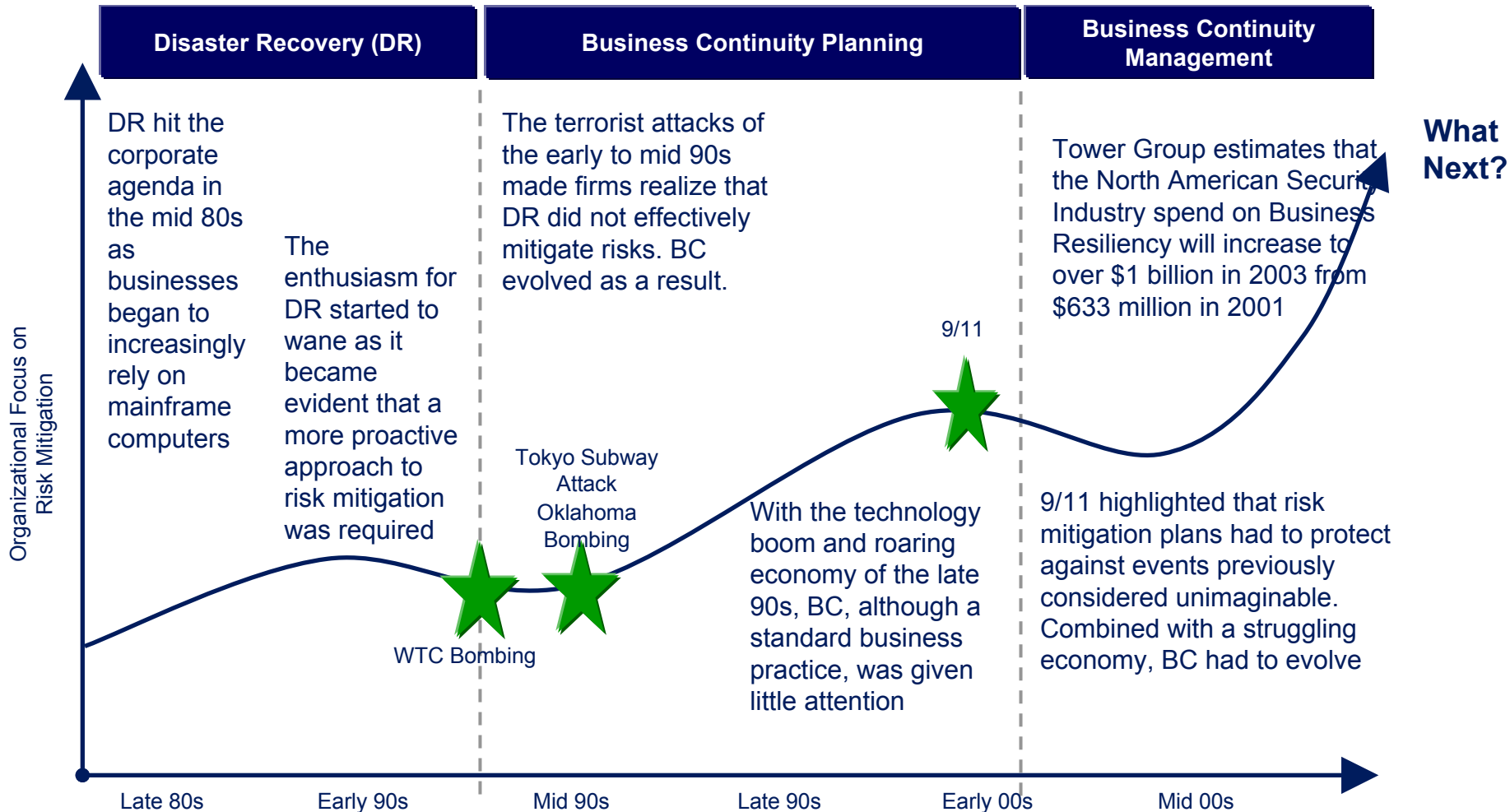
Deloitte.

Background

What is Business Continuity Management?

- A Business Process Driven and IT Supported Program designed to support the viability of an enterprise in the event of significant disruption
- Elements Include
 - Principles of Risk Management
 - Design and implementation of Crisis Management and Emergency Operations Programs
 - Planning for recovery and continued availability of operations during disruptive events
 - Designing and implementing Business Process manual procedures for use during a disruption
 - Designing and implementing secure, fail-proof (fault-tolerant) systems for continuous availability
 - Designing and implementing threat prevention and detection systems
 - Encompasses development of procedures, acquisition of resources, testing and maintenance

The Evolution of Business Continuity



Preparations for crises have evolved from disaster recovery and business continuity planning to a more comprehensive approach called Business Continuity Management

Factors Impacting BCM Today

Increasing Security Threats

- Impact of security incidents is increasing – particularly losses related to theft of proprietary information and denial of service attacks.

The Explosive Growth Of Data

- More data was created from 2000 - 2003 than during the entire history of the Human Race.

The Growing Cost Of Down Time

- Recent estimates put the average cost of down time over \$1,000,000 per hour, with dramatic escalation for companies and processes that are increasingly dependent upon the Internet for eCommerce.

The Increase In Enterprise Applications

- The rapid adoption of enterprise-wide applications, along with an expanding definition of what defines “Mission Critical”, is increasing the demand for more extensive Business Continuity Management.

The Lack of BC/DR Planning

- Opportunities for improvement are multiple – many companies underestimate the importance of BC/DR planning.

Factors Impacting BCM Today

The Uncertain Economy

- Quite rapidly, various factors may converge in an uncertain economy to result in continued pressure on earnings and investment capacity. The challenge is to maintain the right level of resource investment to maintain the viability of Business Continuity Management programs.

Regulatory Requirements

- As is natural in rapidly changing environments, various governing bodies are adding their perspective on the Business Continuity / Disaster Recovery and Security. While some regulations do not specifically detail Business Continuity parameters, there may be far reaching impacts to Continuity Programs (i.e. Sarbanes-Oxley)

Globalization Challenges

- BCM importance grows as businesses operate in a world that continuously grows smaller.

The Unity of Private and Public Efforts

- Both private and public sectors must take part in developing and implementing a collaborative BCM approach in order to unify efforts to cope with emergencies.

Business Continuity Goals



Viability

Keeping the company in business

Earnings/Profit Protection

Protecting the Enterprise' Financial
Commitments

Continuing New Business

Preserving the ability to sell in the marketplace

Brand Protection

Avoiding public embarrassment and loss of
credibility

Business Continuity Objectives

- Provide for safety and well-being of people on premises
- Continue critical business operations
- Minimize immediate damage and losses
- Establish management succession and emergency powers
- Limit financial losses and hardships
- Restore workforce, facilities, and equipment in a timely manner

Business Continuity Priorities

Define priorities in terms of relevance and criticality:

1. Human safety and security issues
2. Preservation of essential data and records, media protection and recovery
3. Protection and restoration of physical equipment
4. Preservation and restoration of the working environment

Business Continuity and Risk Management

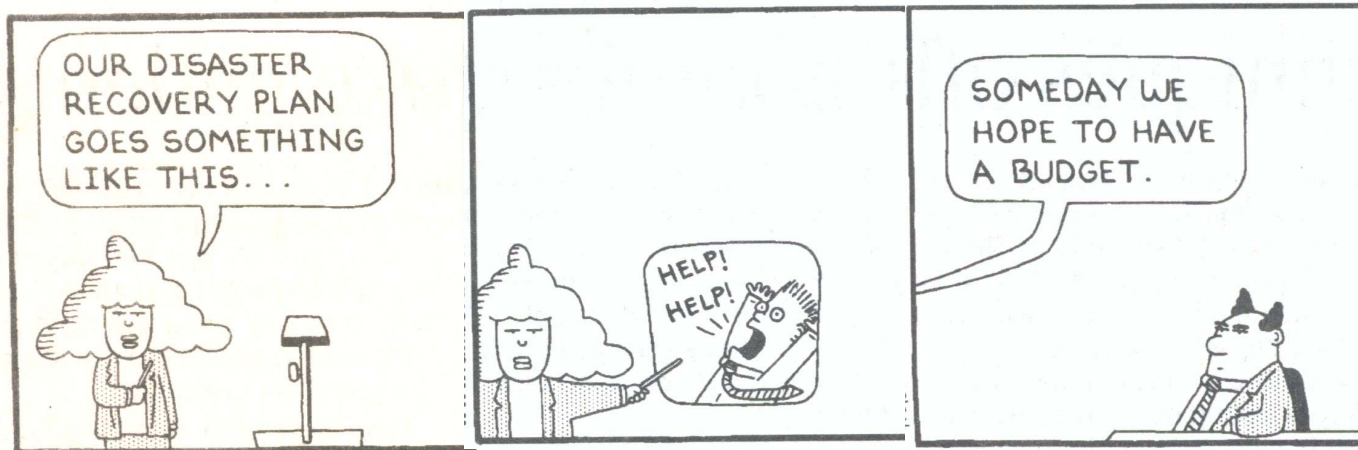
- Business Continuity Management is a part of a comprehensive Risk Management Program
 - Identify exposures to loss
 - Examining the feasibility of alternative risk management techniques
 - Selecting what appears to be the best risk management techniques
 - Implementing the chosen risk management techniques
 - Monitoring, testing, and improving the risk management program

“The ability to define what may happen in the future and to choose amongst alternatives lies at the heart of contemporary society”

**- Peter Bernstein
“Against the Gods”**

What Business Continuity Is Not

- A 'one time project'
- Recovering only Technology (Applications, Hardware)
- A 'Check the Box' Activity to Satisfy Regulatory Requirements
- Something to do to Make Auditors 'Go Away'
- Assuming that Business Survival Can be Achieved, at the Time of Disaster, Using a 'Bunch of Very Smart People'



Business Continuity Challenges

Some issues companies face:

- Insufficient budget for adequate program development and implementation
- Finding knowledgeable resources to manage the program
- Finding internal resources with the time to focus
- Achieving the required cross functional communication and coordination
- Perceived as an expensive “insurance policy”

Terminology and Concepts

Response and Recovery Phases

Emergency Response



**Life-Safety
(Immediate)**



**Damage
Assessment
(24 - 48 Hours)**



**Short-Term
Recovery
(1 Day - 3 Weeks)**



**Long-Term
Recovery
(Months - Years)**

Business Recovery

Crisis Management Components

- Comprehensive coverage includes the following documented procedures:
 - Emergency response and evacuation procedures;
 - Declaration procedures;
 - Executive and employee notification procedures;
 - External communication procedures;
 - Recovery resources and procedures for the mobilization of employees and resources; and
 - Employee responsibilities and action steps for emergency, backup operations, recovery and restoration of operations.

Acronyms

BCP: *Business Continuity Plan*

BCM: *Business Continuity Management*

DRP: *Disaster Recovery Plan*

BRP: *Business Resumption Plan*

BIA: *Business Impact Analysis*

MAO: *Maximum Allowable Outage*

RTO: *Recovery Time Objective*

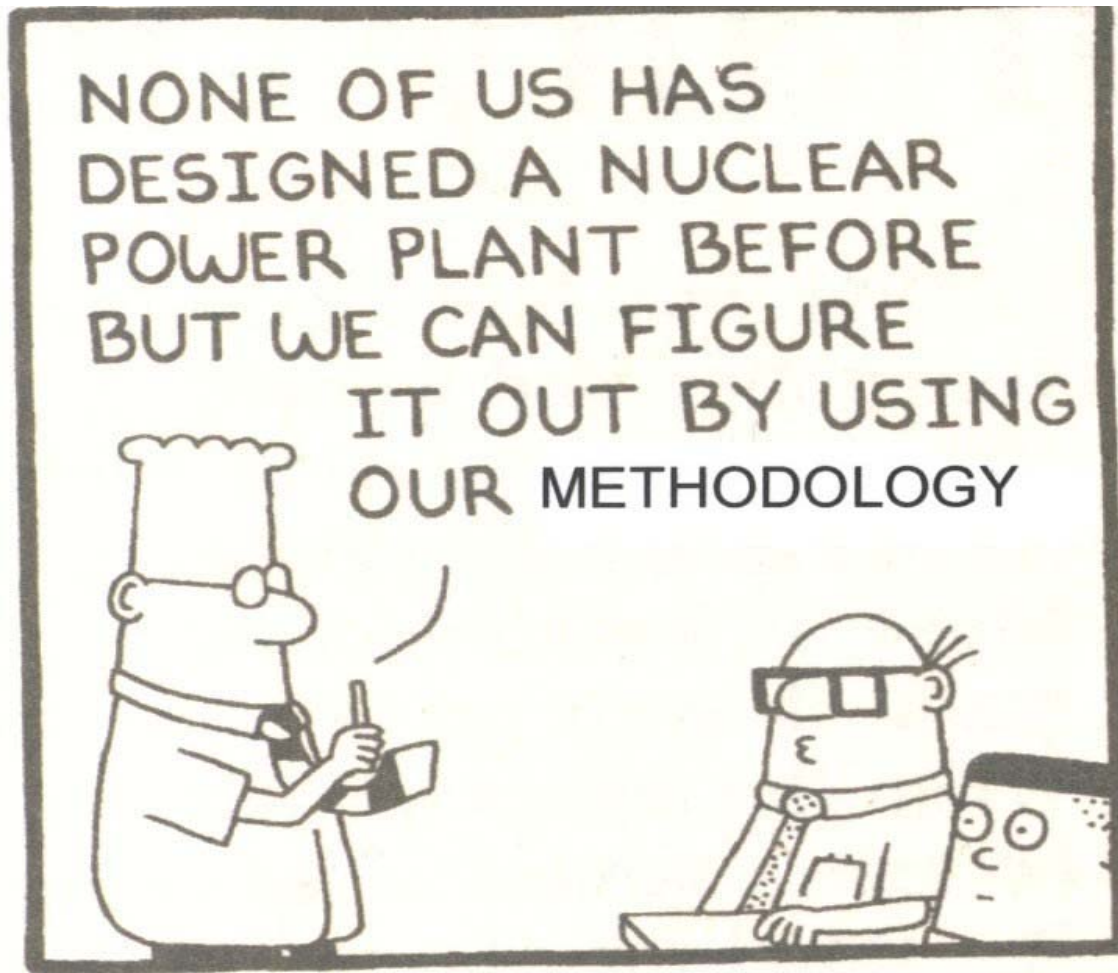
RPO: *Recovery Point Objective*

SPOF: *Single Point of Failure*

Deloitte.

Approach

Of Course We Have A Methodology!



Business Continuity Planning Methodology



Continuous Process Improvement

First Phase: Assessment

The Assessment Phase is composed primarily of requirements and data gathering activities using one or more of the following methods:

- Individual or Group Interviews
- Facilitated Data Gathering Sessions
- Online Tools
- Existing Documentation

Who Will Provide the Data?

- **Steering Committee**
- **Project Sponsor**
- **Business Unit Managers**
- **Key IT Representatives**
- **External ISP/ASP Provider**
- **Other Key Vendors/Suppliers**
- **Building Owner/Management**

Assessment Types



- **Current State Assessment** – What capabilities currently exist to mitigate risks?
- **Risk and Threat Assessment** – What are the key risks and threats to the business processes?
- **Business Impact Analysis** – What are your business's major business processes? What is the impact of disruptions to availability and recoverability?

What is a Current State Assessment?

An Enterprise-Wide Operational Impact Assessment That Analyzes:

- Business Risk
- Operational Impact
- Financial Implications
- External Factors

And Identifies Business Risks, Vulnerabilities, and "Gaps"



- **Hazards**
 - **Internal vs. External**
 - **Natural vs. Man-made**
- **Operational Vulnerabilities**
 - **Critical Functions**
 - **Vital Records**
 - **Key Systems**
- **Business Risks**
 - **Brand Reputation**
 - **Public Perception**
 - **Marketplace Challenges**

Risk and Threat Assessment



- Natural:
 - Floods, earthquakes, tornadoes, etc.
- Human:
 - Man Made – fires, explosions, accidents, bombings, cyber crime, etc.
 - Political – riots, civil disturbances, terrorist attacks, etc.
- Technological:
 - Telecommunications, equipment failure, etc.

Business Impact Analysis (BIA)



- **Business Process Analysis**

- High-level understanding of process flow through interviews with appropriate functional management and documentation review

- **Operational Impact Analysis**

- Define Maximum Allowable Outage (MAO) or Recovery Time Objective (RTO), and Recovery Point Objective (RPO) for each business process

- **Financial Impact Analysis**

- Difficult to quantify and fairly personnel-intrusive
- Only provides "order of magnitude" accuracy over a period of time
- Used for cost-justification of strategy implementation

BIA: Business Process Analysis

- Identify Critical Functions
- Understand Flow of Information, Materials, & Services
- Determine Organizational Dependencies & Resource Needs
- Describe Operational & Financial Impacts of Disruptions
- Define Timeline For Restoring Critical Functions & Critical Data

BIA: Operational Impact Analysis

- Identifies Organizational Implications & Dependencies
- Quantifies Potential Impacts of a Disruption
- Highlights Interrupted Functions & Outage Implications
- Guides Recovery Alternatives Selection

BIA: Financial Impact Analysis

- Quantify Revenue Loss
- Identify Potential Economic Implications
- Include Additional Expenses or Losses
- Evaluate Insurance Strategies
- Help Provide Cost Justification for Recovery Alternatives

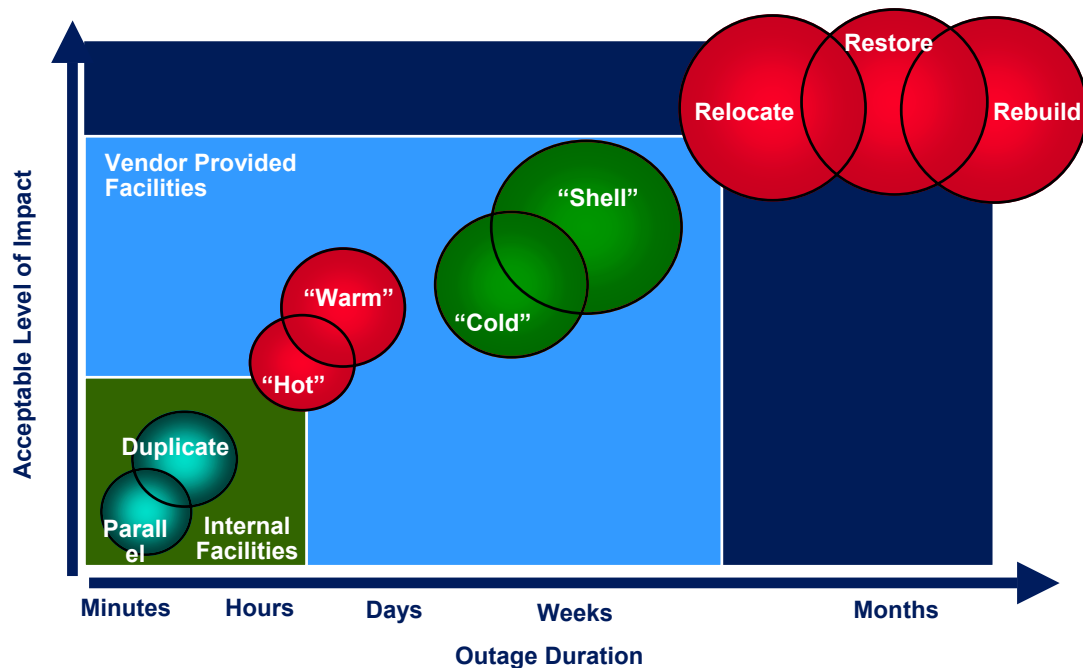
Second Phase: Develop Strategies and Plans



- **Availability Strategies** – Elimination of Single Points of Failure and other enabling strategies
- **Recovery Strategies** – Collaborative design of restoring time critical processes over various periods of time
- **Recovery Plan Documentation** – Business Continuity policies and standards, recovery organization and functional recovery plans

Availability and Recovery Strategies

- Determine Strategy
 - Immediate – Mirroring
 - Next Day – Replication
 - Three Days – Hot Site Contract, etc.
- Focus on Elimination of ‘Single Points of Failure’
- Include Telecoms Recovery Strategies



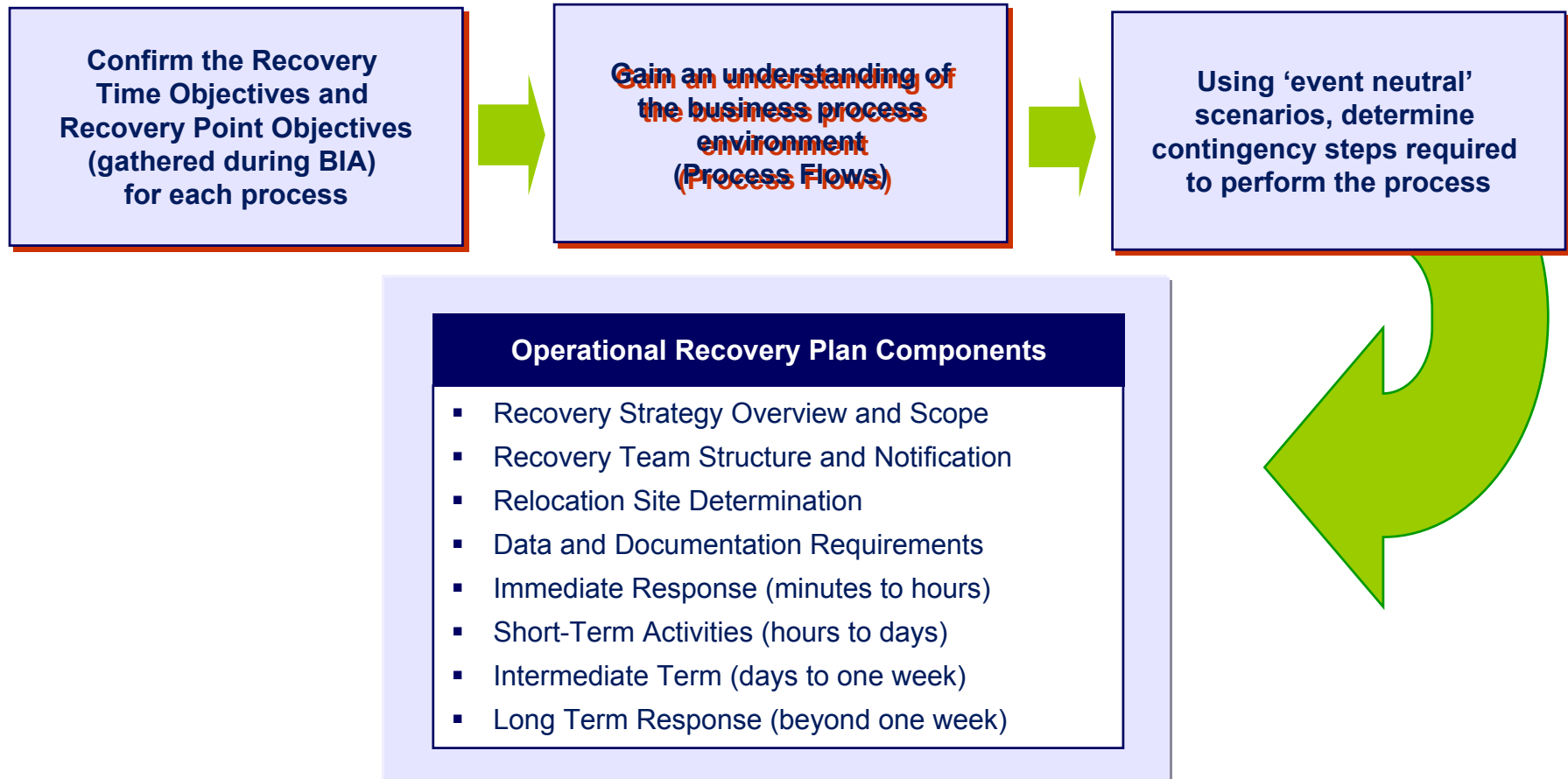
Recovery Strategies: The Emergency Operations Center

The Emergency Operations Center runs the business from disaster declaration to resumption of 'business as usual'.

- **Evacuation**
- **Informing Employees**
- **Tracking Injured and Missing**
- **Notify Families Of Injured**
- **Food & Shelter**
- **Child & Elder Care**
- **Emergency Loans**
- **Temporary Housing**
- **Make Strategic & Policy Decisions**
- **Referred to as "Crisis Management Team"**
- **Composed of Executive Officers, PR, Legal & Support personnel**
- **Communicate With External Stakeholders**
- **Establish Priorities**
- **Provide Direction for Media Releases**
- **Initiate Long-Term Recovery Requirements**
- **Provide Legal Advice**

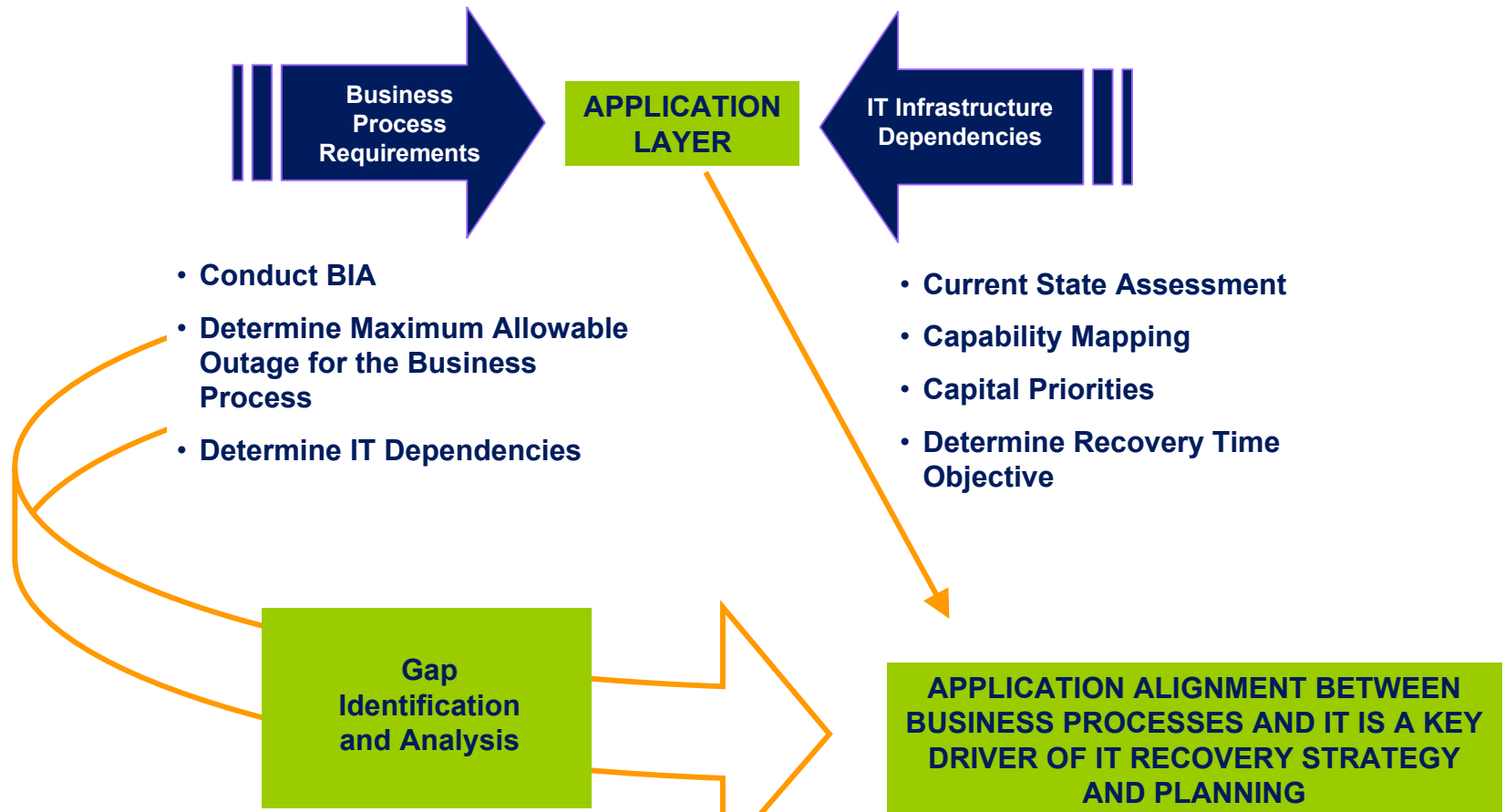
Recovery Plan Documentation: Business Process Recovery

Data from the BIA, existing Operational Recovery Plans and high level process flow diagrams are key inputs to successful plan development



Recovery Plan Documentation: IT Recovery

The application layer connects the business process requirements with technology support. Alignment and understanding of application dependencies is critical to developing the right IT Recovery Plans.



Third Phase: Implementation of the Program

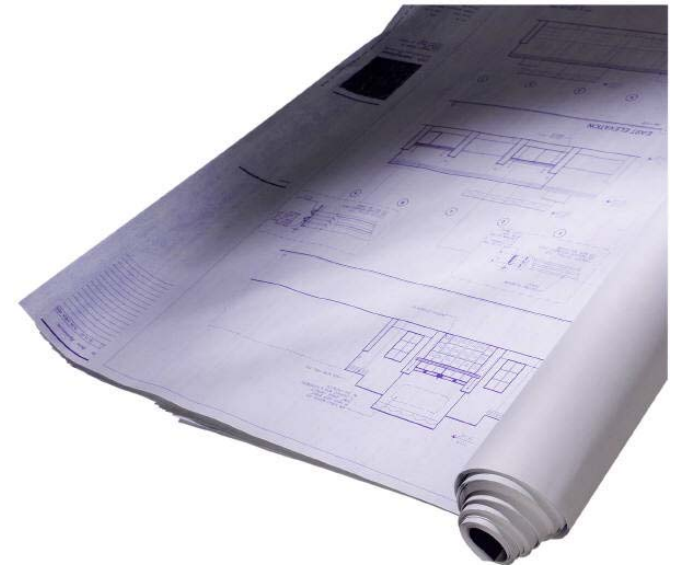


- **Resource Acquisition/Implementation** – Obtaining and implementing the resource requirements to meet strategies and assessment needs
- **Testing/Exercising** – Validate the strategies, usability and readiness of the plans
- **Maintenance/Change Control** – Ensure the strategy, requirements, and plan contents change as organizational and technology changes occur

Resource Acquisition/Implementation

During the Assess and Develop Phases activities that are needed to implement strategies and make recovery plans actionable are identified. The activities are then made into action plans, funding is secured and projects are initiated.

- Management must confirm recovery priorities
- Perform Cost/Benefit Analysis
- Choose the most reasonable course of action
- Manage multiple projects using PMO approach
- Implement the 'quick hits' items first



Testing and Exercising: Overview

- **Increase General Awareness**
- **Reveal Strategy and Resource Gaps**
- **Improve Recovery Coordination**
- **Clarify Roles & Responsibilities**
- **Improve Individual Performance**
- **Motivate Corporate Managers To Support Program**
- **Build Participant Confidence**
- **Foster Cooperation – Public integrated with Private Sectors**



- ✓ **Orientation**
- ✓ **Drills**
- ✓ **Table Top**
- ✓ **Functional**
- ✓ **Fully Integrated**

Testing and Exercising: Elements

- **Define Scope**
- **Develop Purpose & Objectives**
- **Determine Resource Needs**
- **Obtain Commitments for Critical Dates**
- **Develop Scenario, Major Events, Messages**
- **Brief Players, Simulators, Observers**
- **Conduct Exercise**
- **Evaluate Exercise Results**
 - Were the Exercise Objectives Met?
 - Do the Plans Need Improvement?
 - Were there any Training or Staffing Deficiencies?
 - Did Equipment Operate as Expected?

Maintenance/Change Control: Program Governance

Leadership

- What is the overall direction for the business and related IT within the corporation?
- What are the cultural values regarding risk management?
- How should key stakeholders be represented?

Policy

- What should the fundamental BCM operating principles be?
- What internal BCM standards, rules and protocols are needed?

BCM Governance Decisions

Monitoring & Control

- What qualitative benchmarking should be performed?
- How should periodic BCM progress reports be created and reviewed?
- What corrective action should be taken as key findings are made?
- How should the organization ensure corrections take place?

Planning

- What should the corporate business recovery strategy include?
- What should be the corporate IT recovery goals?
- How should BCM program management be measured?

Allocating Capital

- How should limited resources be efficiently allocated?
- What capital is available for investment?
- What criteria should be used to dictate BCM investment decisions?
- What process should be used to review expenditures?

Coordination & Compliance

- What process should be used to ensure compliance with BCM standards and obligations
- How should Corporate BCM coordinate recovery activities between organizational units?

Process Improvement



Process Improvement

- Maintaining the viability and vitality of recovery strategies
- Develop standards and methodologies for ensuring lessons learned are captured
- Plan testing and exercising feedback identify opportunities for plan improvement



Putting It All Together

Putting It All Together...

- Comprehensive plans should combine emergency response and business recovery!
- It is easy to get started if you focus on the right priorities.
- There are reliable techniques for getting executive buy-in.
- Include both a business impact analysis and a risk assessment in the Initial Assessment.

Putting It All Together...

- Before beginning the project, anticipate other costs.
- Using the Incident Command System is critical to “getting back in business” quickly.
- Businesses – Integrate plans with local authorities.
- Public Agencies – Integrate plans with businesses.
- Create the right exercises to test your plans, then follow through with the changes. Then test, test, test again!

