

Business Continuity Plan

enterprise risk management

The Control Professionals

October 2007

Agenda

- Business continuity plan definition
- Evolution of the business continuity plan
- Business continuity plan life cycle
- FFIEC & Business continuity plan
- Questions and answers



Business Continuity Plan Definition

Business continuance (sometimes referred to as *business continuity*) describes the processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster. Business continuance planning seeks to prevent interruption of mission-critical services, and to reestablish full functioning as swiftly and smoothly as possible.

Bitpipe.com 2007

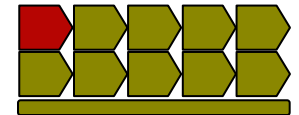
Business Continuity Plan Definition

- Two main Reason why to have a BCP:
 - You need to continue your business
 - It has been made mandatory as part of regulation
- But I have a Disaster Recovery in Place:
 - DR ensures on recovering needed components (usually IT)
 - BCP covers all aspects of being able to continue being in business
 - BCP includes DR

Business Continuity Plan Life Cycle



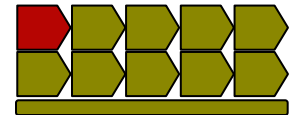
Risk Assessment



Specific objectives:

- Identify the various threats to business continuity
- Assess the company's vulnerability to each threat and the risk exposure
- Review the controls in place to mitigate or reduce risks
- Determine the “**threat scenarios**” for which the continuity strategies and plans should be developed

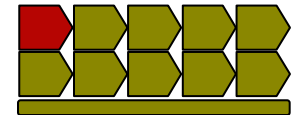
Risk Assessment



There are basically two types of risk assessments:

- **General risk assessment**
 - Identify specific exposures that may warrant further protective measures
- **Business unit risk assessment**
 - Identify functions that have the greatest exposure to interruption, and to identify the resources that the business unit is dependent upon.

Risk Assessment - Threats



Floods, Hurricanes, Tornadoes, Electric storms

Fire, Power failure, Loss of access, Explosion

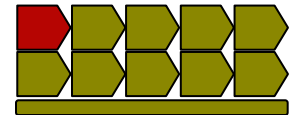
Strikes, Epidemics, Loss of key personnel

Viruses, Hacking, Hardware failure, Data loss

Bad Publicity, Financial crisis, Regulatory issues

Riots, Protests, Bomb threats, Terrorism

Risk Assessment - Results



General risk assessment

- Matrix of resources each function upon, showing extent of the dependency (low, moderate, high)

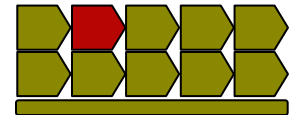
Business unit risk assessment

- List of threats, showing criticality level, coverage, and a calculated risk exposure.

Business

- Ranking of each function's overall, exposure interruption.
- Ranking of the business unit's exposure to interruption by potential threat.

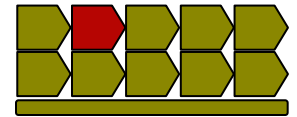
Business Impact Analysis



Specific objectives:

- Identify critical business unit functions based on the consequences of a threat event occurs
- Establish the maximum length of time each function can be suspended in a crisis situation
- Determine minimum resources required to resume each essential function
- Define recovery requirements for essential computer systems and data
- Determine priorities for system recovery and business resumption

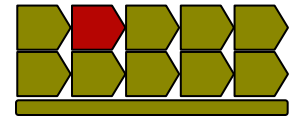
Business Impact Analysis



There are different types of Business Impact Analysis:

- **Threat scenario impact analysis**
 - The overall impacts are assessed for each ‘threat scenario’ identified during the risk assessment
- **Technology impact analysis**
 - The time-dependent impact of loss of specific technologies or computer system is assessed across the organization
 - Principal objective is to determine the maximum downtimes for various technologies and the maximum data loss that can be tolerated
- **Business unit impact analysis**
 - The time-dependent impacts of an interruption in operations is assessed for each business unit
 - The primary objectives are to identify all essential functions, and to determine the maximum downtime for each function
 - The secondary objectives are to determine the minimum resources required to perform each function at an acceptable level, and to establish priorities for resumption of operations

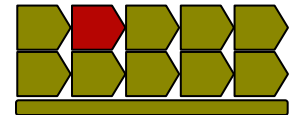
Business Impact Analysis



Key Terms:

- **Recovery Time Objective (RTO) (time to recover)**
 - The shorter the RTO, the more expensive the strategy
 - The longer the RTO, the more time you have to resolve the situation
 - It is possible to have multiples RTO per mission function
- **Recovery Point Objective (RPO)(time to recover relative to disaster)**
 - Used as the basis for the development of data backup strategies
 - If RPO equal 0, no data loss

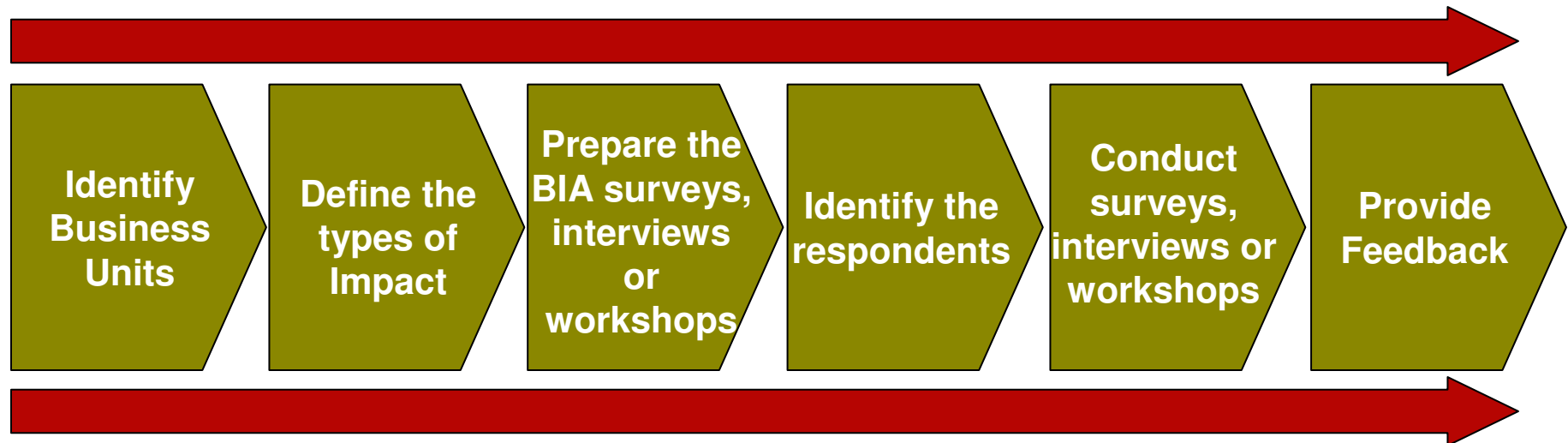
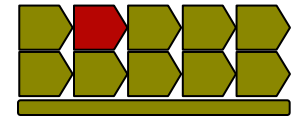
Business Impact Analysis



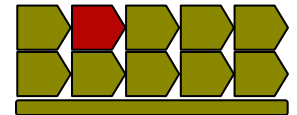
Key Terms:

- **Maximum Tolerable Downtime (MTD) or Maximum Allowable Downtime (MAD)**
 - Used as a determinant as to whether activate the BCP for a specific event
 - The RTO for the function and supporting systems and technologies, cannot be greater than the MTD/MAD

Business Impact Analysis - Steps



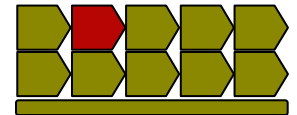
Business Impact Analysis



Following are some typical questions that need to be answered during the business impact analysis:

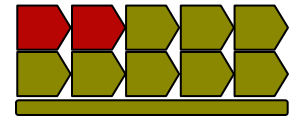
- What are the major functions performed at each of the company's locations?
- What are the approximate staffing levels for each function?
- What computer systems or services are required to perform each function?
- How long could each system or service be unavailable before the impacts reached unacceptable levels?
- What vital records are used or maintained by each function?
- How long could each function be suspended before the impacts reached unacceptable levels?
- Are there any existing contingency measures that could be utilized to avoid or delay potential impacts, or reduce their severity?

Business Impact Analysis - Results



- List of impact categories with weighting factors
- Parameters defining severity of impact
- List of business units functions with a brief description and impact summaries
- Impact timelines by business unit function
- Impact scorecard (impact ratings X weighting factors)
- Prioritization of business unit functions and establishment of maximum tolerable downtime for each function
- Resources requirements by business unit function

Risk Assessment / Business Impact Analysis Techniques

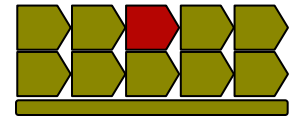


There are several techniques that can be used to gather information for the risk assessment and the business impact analysis:

- Interviews
- Workshops
- Surveys or templates



Continuity Strategy Section

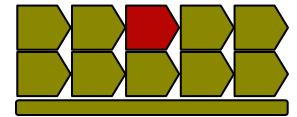


This phase has two steps:

1 - Analyzing the data and determining options

- Start with the 'quick hits' identified in the risk assessment and business impact analysis
- Address the 'single points of failures'
- Identify the options for recovering computer systems and data, and resuming operations, in the event of a disaster
- Evaluate the options (internal and external)

Continuity Strategy Section

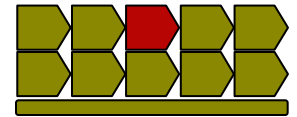


2 - Identifying strategies to reduce risk and impact

Based on the information gathered in the previous phases and step, the strategy should be identified, selected, and implemented for:

- Reduce risk
- Reduce impact
- Recovering computers
- Resuming business operations

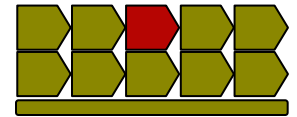
Computer Recovery Strategies



There are four basic components to recovery strategies for computer systems:

- Location
- Connectivity
- Hardware
- Backups

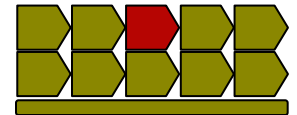
Business Resumption Strategies



There are five basic components to strategies for resuming business operations:

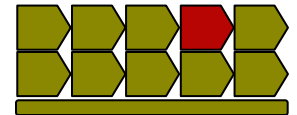
- Location
- Connectivity
- Workstations
- Equipment & Materials
- Staff

Continuity Strategy Section



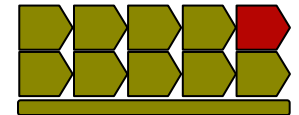
- Selecting the right business continuity strategy usually involves trade-offs. The most effective strategy is the most expensive. In controversy, the least expensive strategy is often impractical, risky, or fails to meet operational requirements
- The challenge is to identify those strategies that are affordable but will provide an appropriate level of risk management

Computer Recovery Plan Development



- The traditional goal of Disaster Recovery Plan is to recover computer systems from “bare metal” in the event of disastrous incident.
- The systems to be recovered may include:
 - Mainframes systems
 - Mid-range systems
 - Client/server systems
- Typically challenges to recovery include:
 - Volumes of data
 - Synchronization of data and systems
 - Number and types of hardware devices
 - Lack of standardization
- Recovery procedures must be well documented, tested, and maintained

Incident Management Plan Development



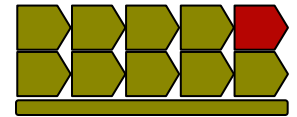
The main objective of this phase is:

Develop plans for resuming critical business functions, which include:

- Resource requirements definition
- Team member contact information
- Activity lists
- Detailed activity documentation
- Off-site material list, etc.

An incident Management Plan is a documented series of activities that may need to be performed by designated BCP Teams in response to a potentially disastrous incident.

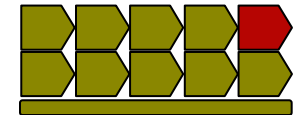
Incident Management Plan Development



The incident Management Plan should contain:

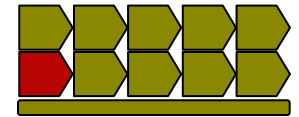
- Strategic overview of each incident type
- List of minimum recovery requirements
- Team membership and contact information
- Off-site materials list and other supporting documents
- Activity lists organized by phase and scenario
- Activity details

Incident Management Plan - Phases

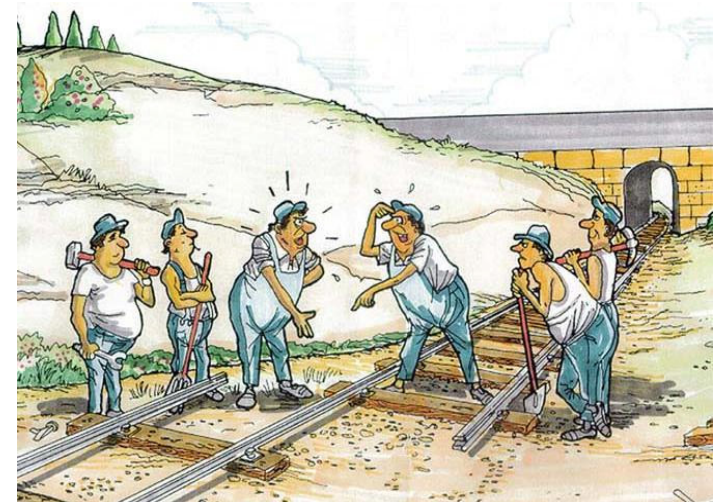


Phases Definition	
Initial Assessment and response	Assess the impact of the event on operations
Interim Contingency Measures	Implement short term measures to limit the impact of the event
Resource Provisioning	Provide the minimum resources need to resume operations
Operations Resumption	Resume an acceptable level of operations
Reconstitution	Complete all actions required to resolve the event

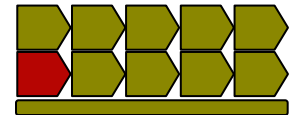
Establish Teams



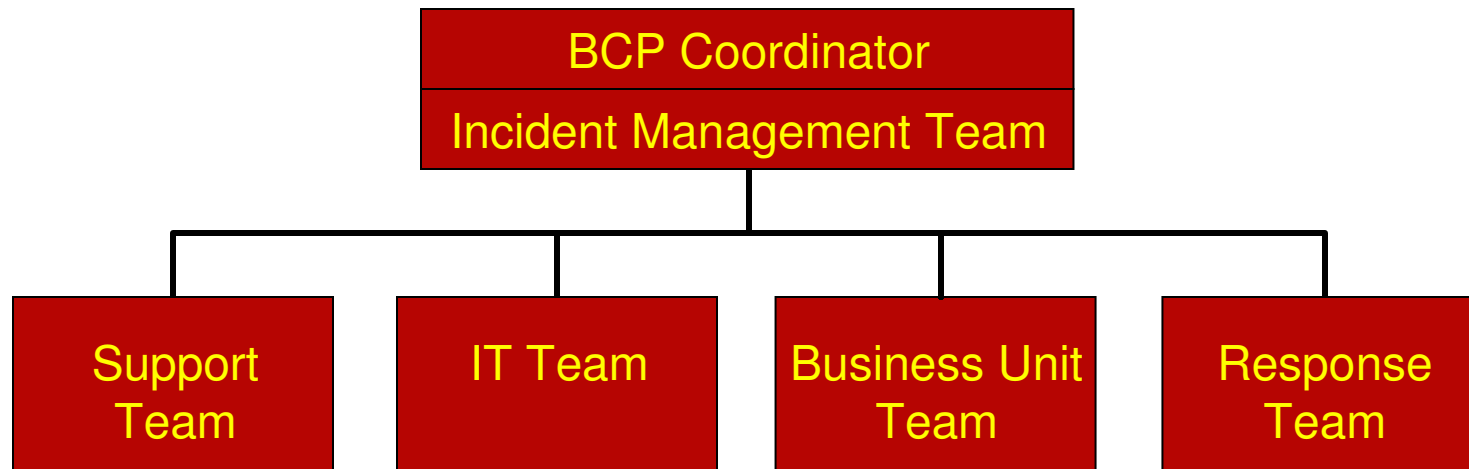
No matter how well designed or documented the BCP plans, it will be useless unless there are people who know how to execute those plans



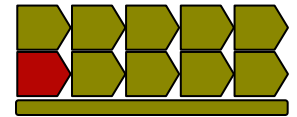
Establish Teams – Team Structure



Typical team structure



Establish Teams – Team Structure



Incident Management Team

- Designated group of senior individuals responsible for overall management of a potentially disastrous event

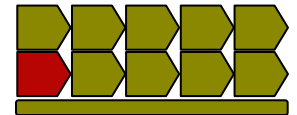
Response Team

- Group of individuals who would be activated immediately if an emergency event occurs at any company facility. They are typically facilities and/or security personnel.

Business Unit Team

- Group of individuals who coordinate the activities of a specific business unit or functional area following the incident. They are typically the front line managers.

Establish Teams – Team Structure



Information Technology Team

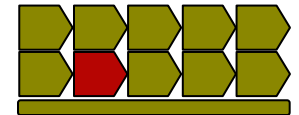
- Group of specialists that would restore the technology infrastructure, computer systems, or electronic data.

Support Team

- Specialized group that would help manage the various activities necessitated by the accident.



Implement Incident Management Framework

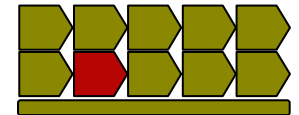


The main objective of this phase is the implementation of a framework for managing an incident, including:

- Emergency response procedures
- Communication procedures
- Decision-making criteria
- Management succession
- Human resources policies



Implement Incident Management Framework



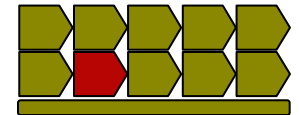
Managing a major incident or crisis is not the same as responding to an emergency.

Emergency – Short term event requiring immediate, predetermined actions

Major incident or crisis – Long term event requiring planning and coordinated execution of many independent activities

Emergency response is **tactical**; Incident management is **strategic**

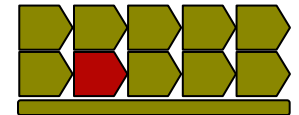
Implement Incident Management Framework



The ability to manage a major incident or crisis effectively requires:

- Appointment of an Incident Management Team
- Procedures for escalation of an emergency, and notification of the team members
- Procedures for activation of BCP teams and plans
- Incident management checklist

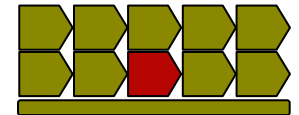
Implement Incident Management Framework



Key areas may need to be addressed in an incident management plan:

- Decision-making authority and criteria
- Succession planning
- Coordination with public authorities
- Human resources issues
- Financial control issues
- Legal, contractual and regulatory issues
- Crisis communications

Awareness and Training



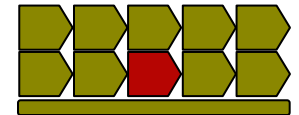
Importance of people in the BCP

– People

- select the Plan
- update the Plan
- test the Plan
- **execute** the Plan

Involved personnel should understand, follow and practice the BCP

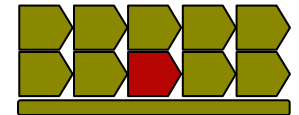
Awareness and Training



Proper awareness can be used to

- Communicate policies, standards, and methodologies to be followed within the BCP
- Identify any needed and/or further training requirements for the personnel involved in the BCP execution
- Avoid misunderstandings and confusion
- Continuously reinforce the BCP key elements and concepts
- Facilitate the learning process of the BCP and increase the level of knowledge and participation

Awareness and Training



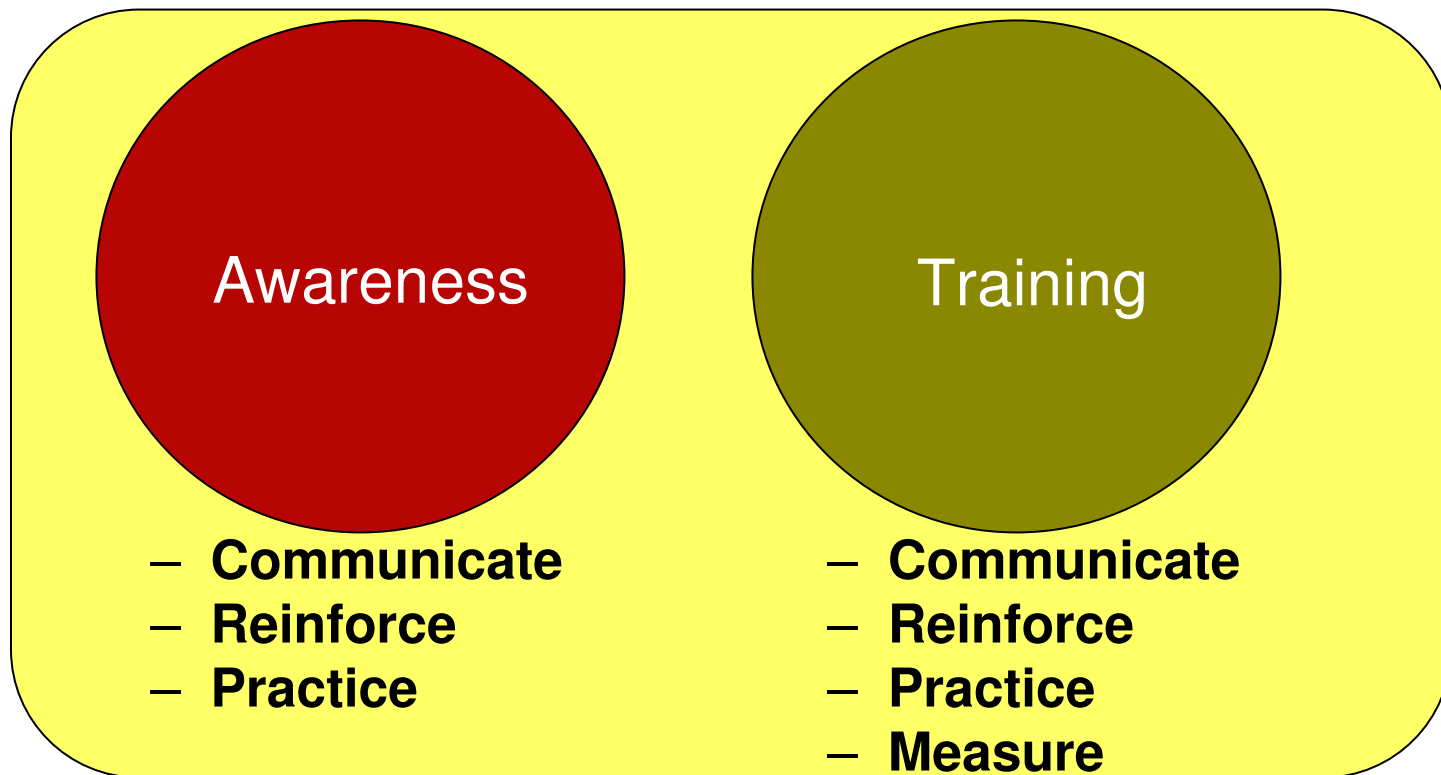
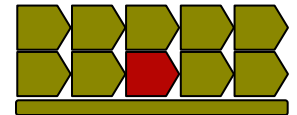
Awareness

Awareness is having knowledge or being conscious of certain information
Objective is to **KNOW** something

Training

Testing is putting to practice and improving a particular skill or model of behavior
Objective is to **KNOW HOW TO DO** something

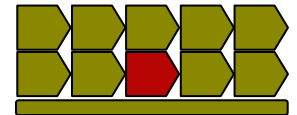
Awareness and Training



Practice is the main difference between the two

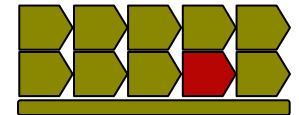
Awareness and Training

To design an effective awareness and training program, you first need to determine:



Who	<i>The target audience is</i>
What	<i>You want them to know, and know how to do</i>
Why	<i>You want them to know</i>

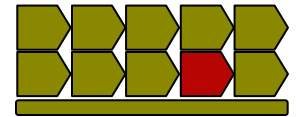
Testing and Exercising



Business continuity plans require regular testing and validation

- **Testing** – It an activity that is performed to evaluate performance, capabilities or properties relative to specified measurement criteria
- **Validation** – It an activity that is performed with the purpose of corroborating soundness, completeness, or effectiveness

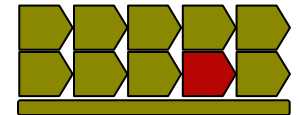
Testing and Exercising



What you should Test?

- All manual procedures
- All automated procedures
- All backups and recovery configurations
- All call trees
- All contact lists, resources list, off-site inventory lists, etc.

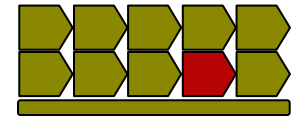
Testing and Exercising



When should you Test?

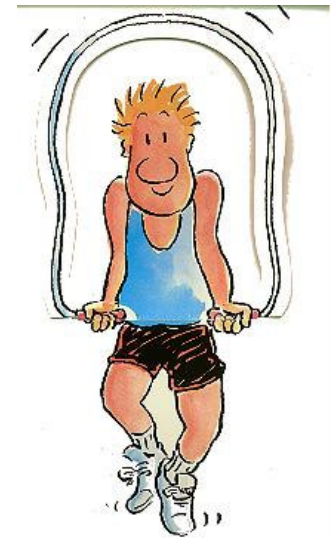
- Every component should be tested **annually**
- Critical and/or highly volatile components should be tested at **least quarterly** and after any major technology change
- Call trees should be tested at **least semiannually**
- Components which fails the test should be tested **as soon as possible**

Testing and Exercising

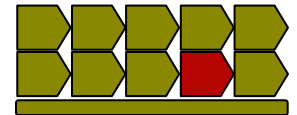


How should you test?

- Desk check
- Peer review
- Structured walkthrough
- Call tree test
- Standalone operational test
- Integrated operational test
- Operation stress test
- Parallel operational test
- Live operational test



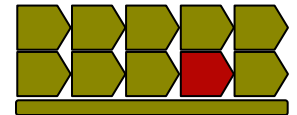
Testing and Exercising



How should you measure success?

- Test results should be compared to predefined measurement criteria
- Metrics should be defined for every test, and an objective process for assessing levels of success established before the test
- Scored should be completed after each test and retained for comparison with future results
- There is often reluctance to treat any test as a failure, or to quantify the level of success - **Serious Mistake** -

Testing and Exercising

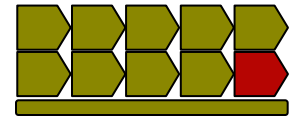


Regardless of how well you may have **tested** your plans, they may not work as expected unless you regularly **exercise** your BCP team

Types of exercises:

- Orientation seminars
- Drills
- Tabletop exercise
- Functional exercise
- Full-scale exercise
- Mock disaster

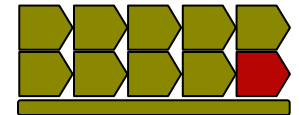
Maintenance and Evaluation



The main object of this phase is to establish an on-going process:

- Updating plan contents
- Distributing plan updates
- Controlling plan access
- Evaluating plan effectiveness
- Auditing BCP processes
- Maintaining contracts, etc

Maintenance and Evaluation



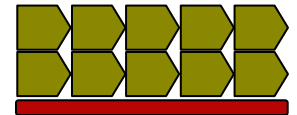
Plan maintenance

The process of updating, on timely basis, any components of the plan that have been affected by organizational, technological, or business change

Plan administration

The process of protecting the confidentiality, integrity, availability of the BCP Plan; controlling and distributing plan updates; managing service contracts; etc.

Program Management



Establish a permanent framework for managing the on-going program:

- Issue policies and standards
- Assign accountability
- Create a steering committee
- Set annual budgets and objectives
- Monitor and enforce compliance

FFIEC & Business Continuity Plan

The FFIEC agencies encourage financial institutions to adopt a process-oriented approach to business continuity planning that involves:

- Business Impact Analysis (BIA)
- Risk Assessment
- Risk Management
- Risk Monitoring

FFIEC & Business Continuity Plan

Business Impact Analysis (BIA)

- Identification of the potential impact of uncontrolled, non-specific events on the institution's business processes and its customers
- Estimation of maximum allowable downtime and acceptable levels of data, operations, and financial losses.

Risk Assessment

- Prioritizing of potential business disruptions based upon severity and likelihood of occurrence
- A gap analysis comparing with the institution's existing BCP
- Analysis of threats based upon the impact on the institution, its customers, and the financial markets, not just the nature of the threat

FFIEC & Business Continuity Plan

Risk Management

The institution should ensure that the BCP is:

- Written and disseminated so that various groups of personnel can implement it in a timely manner
- Specific regarding what conditions should prompt implementation of the plan
- Specific regarding what immediate steps should be taken during a disruption
- Flexible to respond to unanticipated threat scenarios and changing internal conditions
- Focused on how to get the business up and running in the event that a specific facility or function is disrupted, rather than on the precise nature of the disruption
- Effective in minimizing services disruptions and financial loss

FFIEC & Business Continuity Plan

Risk Monitoring

- Test the BCP at least annually
- Subjecting the BCP to independent audit and review
- Updating the BCP based upon changes to personnel and the internal and external environment

Questions ?



Contact Information

Enterprise Risk Management

Phone: 305.447.6750

Mobile: 305.335.7610

Fax: 305.447.6752

e-mail: **info@emrisk.com**

URL: **www.emrisk.com**