Business Continuity Planning 101

Presented by Strohl Systems

We will begin shortly.
Thank you for your patience.

STROHL SYSTEMS

Business Continuity Planning 101

Gretchen Hertzog, ABCP

Product Specialist

Strohl Systems

Presentation Overview

- What is business continuity planning
- FFIEC/NCUA regulations for BCP
- Plan Development
- Plan Testing
- Plan Maintenance
- Future advancements in BCP
- Question & Answer

What is a Disaster?

- A disaster is a sudden, unplanned calamitous event that creates the **inability to provide the critical business functions** for some predetermined period of time and which results in great damage or loss
  (DRI International)

- The **time factor** which determines whether a service interruption is an *inconvenience* or a *disaster* will vary from organization to organization

Disasters are never on our calendar However, we can prepare for them

What is Business Continuity Planning?

- An **on-going**, coordinated program of strategies, plans and procedures
  - Ensures critical resources are available in the event of a physical disruption to any part of the business
  - Changes along with your business
- Business continuity **bridges the gap** between disaster and recovery
- Business continuity identifies weak links in the flow of information & establishes procedures to **eliminate downtime**

Business Continuity vs. Disaster Recovery

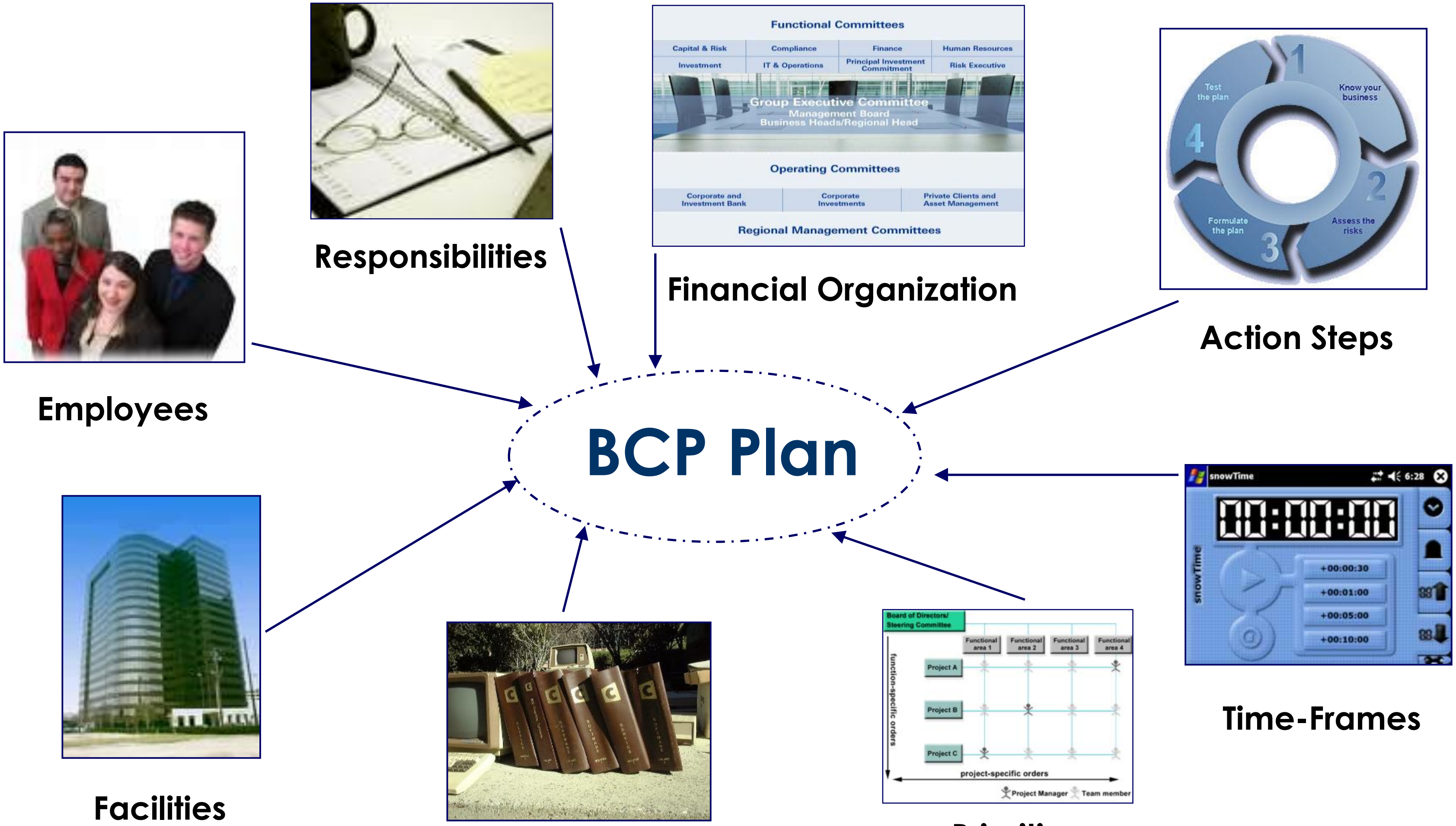
- **Business Continuity Planning**
  - Proactive Process
  - Helps to prevent interruption of mission critical services
  - Global - covers most or all of an organization’s critical business processes and operations

- **Disaster Recovery Planning**
  - Reactive Process
  - Technical plans that are developed to recover a specific business application
  - Focuses include IT, call centers, and distribution centers

The Goal of BCP

- Protect your **PEOPLE**
- Define **service alternatives** for accomplishing critical applications
- **Minimize** the extent of interruption
- Limit **financial losses** and hardships
- Establish customer **confidence**
- Satisfy federal and state **compliance regulations**

What’s in a Business Continuity Plan?



Compliance Elements of BCP

- **Keep Plan up-to-date**
  - Plan changes should reflect organizational changes
- **Assure processes reflect business needs**
  - Modify processes and procedures accordingly
- **On-going training**
  - For all new and existing employees
- **Trained Recovery Teams**
  - Members of recovery teams must be aware of responsibilities

Event

RESPONSE

- Assessment
- Escalation
- Declaration

RESUMPTION

- Initial Phase
- Short-term Continuity
- Most Critical Services

RECOVERY & RESTORATION

- Long-term Continuity
- Repair/ Replace
- Migration
- Resume “Normal” Service

FFIEC & NCUA Regulation Changes

- Reasons for major regulation changes in 2004:
  - Organizations face **new threats**
  - Organizations have higher dependency on **new technology**

- As a result:
  - More regulatory focus on **Business Resumption**
  - Greater emphasis on Plan **Testing and Maintenance**

Why New Requirements for BCP?

- Old Assumptions – **No longer valid** in planning
- **New Perspectives** – Necessary for comprehensive planning
- Requirement for **enterprise-wide** planning
- **Recovery time objectives** – becoming shorter and shorter
- **Interdependency** within business processes
- **Technology** dependence outside the organization

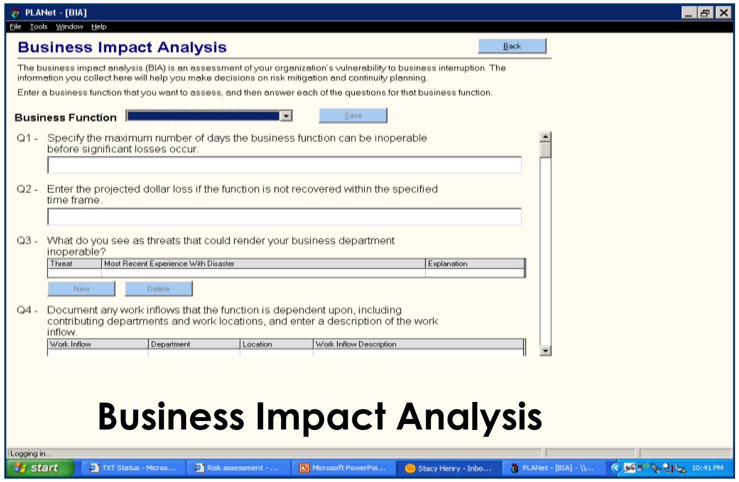
Source: FFIEC IT Handbook Presentation

BOD & Senior Management

Responsibilities include:

- Allocating sufficient resources and knowledgeable personnel to development of BCP
- Setting policy by determining how the institution will manage and control identified risks
- Reviewing BCP test results and approving the plan on an annual basis
- Ensuring maintenance of BCP and training all employees
- Reviewing Insurance
- Coordinating with local Emergency Response Units for BCP

Essential Components for Compliance



Business Impact Analysis

The business impact analysis (BIA) is an assessment of your organization's vulnerability to business interruption. The information you collect here will help you make decisions on risk mitigation and continuity planning.

Enter a business function that you want to assess, and then answer each of the questions for that business function.

Business Function

Q1 - Specify the maximum number of days the business function can be inoperable before significant losses occur.

Q2 - Enter the projected dollar loss if the function is not recovered within the specified time frame.

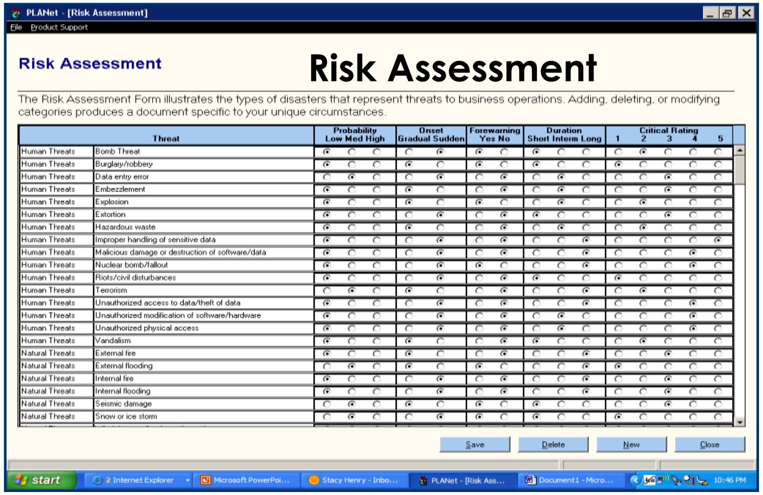
Q3 - What do you see as threats that could render your business department inoperable?

Threat	Most Recent Experience With Disaster	Explanation

Q4 - Document any work inflows that the function is dependent upon, including contributing departments and work locations, and enter a description of the work inflow.

Work Inflow	Department	Location	Work Inflow Description

Business Impact Analysis

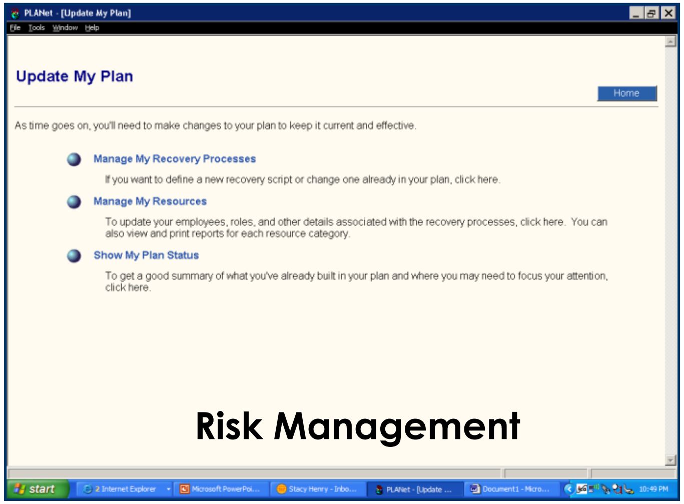


Risk Assessment

Risk Assessment

The Risk Assessment Form illustrates the types of disasters that represent threats to business operations. Adding, deleting, or modifying categories produces a document specific to your unique circumstances.

Threat		Probability			Onset		Forewarning		Duration			Critical Rating				
		Low	Med	High	Gradual	Sudden	Yes	No	Short	Interm	Long	1	2	3	4	5
Human Threats	Bomb Threat	●	○	○	○	●	●	○	●	○	○	○	●	○	○	○
Human Threats	Burglary/robbery	●	○	○	●	○	●	○	●	○	○	●	○	○	○	○
Human Threats	Data entry error	○	●	○	○	●	○	●	○	●	○	○	○	●	○	○
Human Threats	Embezzlement	●	○	○	●	○	○	●	○	●	○	○	○	●	○	○
Human Threats	Explosion	●	○	○	●	○	●	○	○	●	○	○	●	○	○	○
Human Threats	Extortion	●	○	○	○	●	○	●	●	○	○	○	○	●	○	○
Human Threats	Hazardous waste	●	○	○	●	○	○	●	○	●	○	○	●	○	○	○
Human Threats	Improper handling of sensitive data	●	○	○	○	●	○	●	○	○	●	○	○	○	○	●
Human Threats	Malicious damage or destruction of software/data	●	○	○	○	●	○	●	○	○	●	○	○	○	●	○
Human Threats	Nuclear bomb/fallout	●	○	○	○	●	●	○	○	○	●	○	○	○	●	○
Human Threats	Riots/civil disturbances	●	○	○	○	●	○	●	●	○	○	●	○	○	○	○
Human Threats	Terrorism	○	●	○	●	○	○	●	○	○	●	○	●	○	○	○
Human Threats	Unauthorized access to data/theft of data	●	○	○	○	●	○	●	○	○	●	○	○	○	●	○
Human Threats	Unauthorized modification of software/hardware	●	○	○	○	●	○	●	○	●	○	○	○	○	●	○
Human Threats	Unauthorized physical access	●	○	○	○	●	○	●	○	●	○	○	○	○	●	○
Human Threats	Vandalism	●	○	○	●	○	○	●	●	○	○	○	●	○	○	○
Natural Threats	External fire	●	○	○	●	○	○	●	○	○	●	○	○	●	○	○
Natural Threats	External flooding	○	●	○	●	○	●	○	○	○	●	●	○	○	○	○
Natural Threats	Internal fire	●	○	○	○	●	○	●	○	○	●	○	○	●	○	○
Natural Threats	Internal flooding	●	○	○	○	●	○	●	○	○	●	○	○	●	○	○
Natural Threats	Seismic damage	○	●	○	●	○	●	○	●	○	○	○	○	●	○	○
Natural Threats	Snow or ice storm	○	●	○	○	●	●	○	●	○	○	●	○	○	○	○

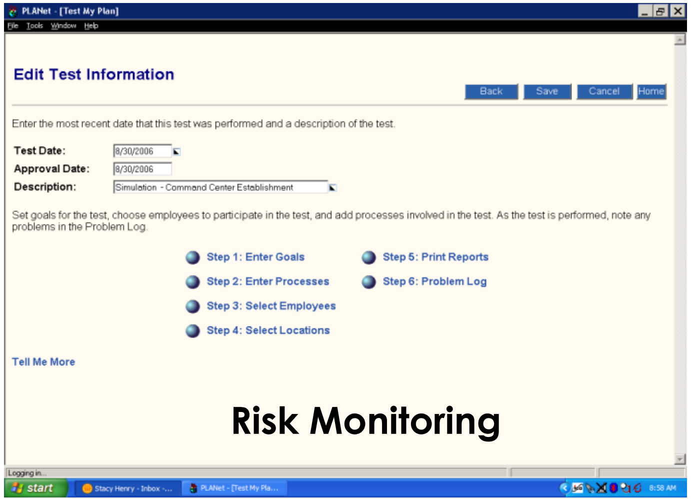


Update My Plan

As time goes on, you'll need to make changes to your plan to keep it current and effective.

- **Manage My Recovery Processes**
  If you want to define a new recovery script or change one already in your plan, click here.
- **Manage My Resources**
  To update your employees, roles, and other details associated with the recovery processes, click here. You can also view and print reports for each resource category.
- **Show My Plan Status**
  To get a good summary of what you've already built in your plan and where you may need to focus your attention, click here.

Risk Management



Edit Test Information

Enter the most recent date that this test was performed and a description of the test.

Test Date: 8/30/2006
Approval Date: 8/30/2006
Description: Simulation - Command Center Establishment

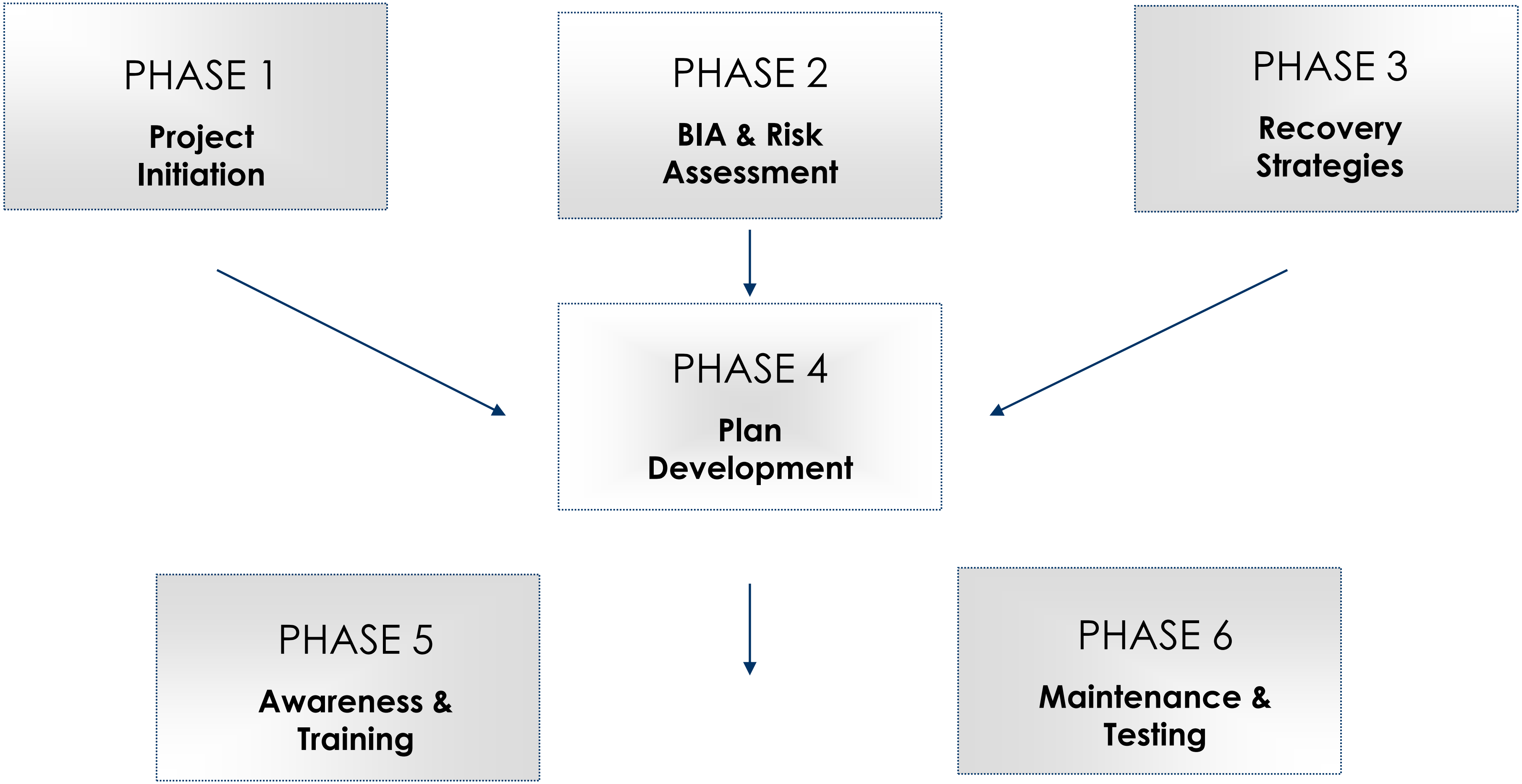
Set goals for the test, choose employees to participate in the test, and add processes involved in the test. As the test is performed, note any problems in the Problem Log.

- Step 1: Enter Goals
- Step 2: Enter Processes
- Step 3: Select Employees
- Step 4: Select Locations
- Step 5: Print Reports
- Step 6: Problem Log

Tell Me More

Risk Monitoring

A Project Approach To Planning



PHASE 1

Project Initiation

PHASE 2

BIA & Risk Assessment

PHASE 3

Recovery Strategies

PHASE 4

Plan Development

PHASE 5

Awareness & Training

PHASE 6

Maintenance & Testing

Phase 1 – Project Initiation

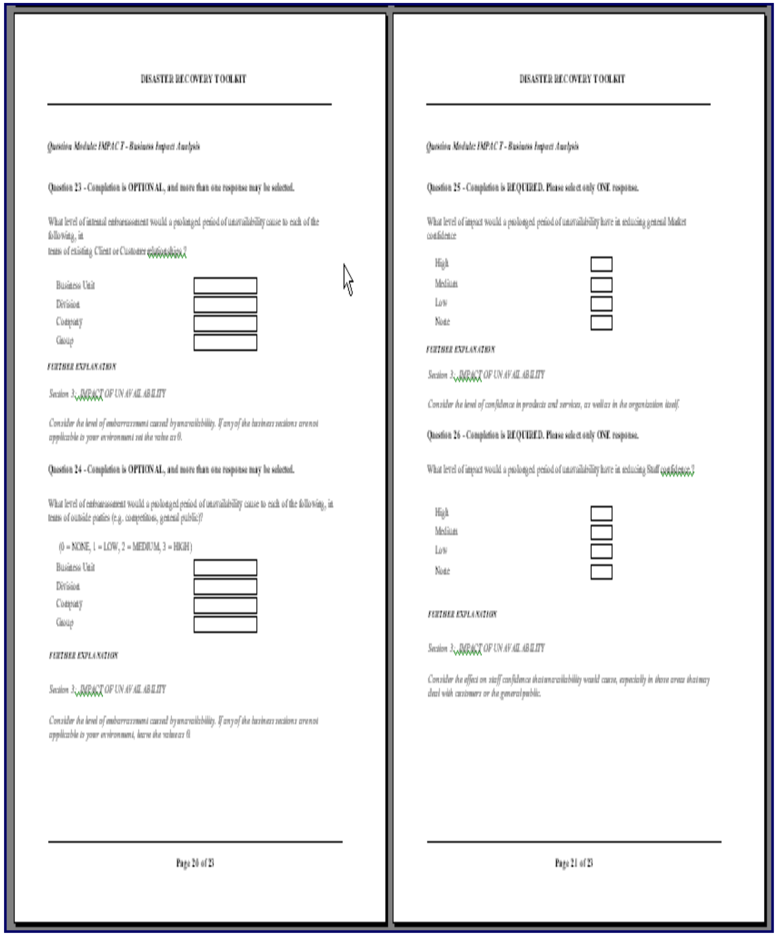
- Gain Senior Management Support
- Define terms, objectives and assumptions
- Assign responsibility and accountability
- Familiarize Team Leaders and participants with the planning process and resource requirements
- Provide a roadmap of the project with projections

Phase 2 – Business Impact Analysis

- **Required** for FFIEC & NCUA compliance
- **BIA is the foundation** of all Business Continuity Programs
- Detailed analysis of **all business functions & processes**
- Aids in determining the potential impact of a disruption
  - **Quantitative Impact** – monetary loss
  - **Qualitative Impact** – intangible loss
- Information gathered will help to:
  - **Prioritize** business units & critical processes
  - Define **interdependencies** within organization

Approach to BIA

- Define scope & assumptions
- Develop a survey to gather necessary information
- Identify & notify appropriate recipients
- Distribute survey
- Analyze data and verify results
- Present findings
- Make joint decisions on risk mitigation



DISASTER RECOVERY TOOLKIT

Question Module: IMPACT - Business Impact Analysis

Question 23 - Completion is OPTIONAL, and more than one response may be selected.

What level of internal embarrassment would a prolonged period of unavailability cause to each of the following, in
terms of existing Client or Customer relationships?

Business Unit	
Division	
Company	
Group	

FURTHER EXPLANATION

Section 3: IMPACT OF UNAVAILABILITY

Consider the level of embarrassment caused by unavailability. If any of the business sections are not applicable to your environment set the value as 0.

Question 24 - Completion is OPTIONAL, and more than one response may be selected.

What level of embarrassment would a prolonged period of unavailability cause to each of the following, in terms of outside parties (e.g. competitors, general public)?

(0 = NONE, 1 = LOW, 2 = MEDIUM, 3 = HIGH)

Business Unit	
Division	
Company	
Group	

FURTHER EXPLANATION

Section 3: IMPACT OF UNAVAILABILITY

Consider the level of embarrassment caused by unavailability. If any of the business sections are not applicable to your environment, leave the value as 0.

Page 20 of 23

DISASTER RECOVERY TOOLKIT

Question Module: IMPACT - Business Impact Analysis

Question 25 - Completion is REQUIRED. Please select only ONE response.

What level of impact would a prolonged period of unavailability have in reducing general Market confidence

High □
Medium □
Low □
None □

FURTHER EXPLANATION

Section 3: IMPACT OF UNAVAILABILITY

Consider the level of confidence in products and services, as well as in the organization itself.

Question 26 - Completion is REQUIRED. Please select only ONE response.

What level of impact would a prolonged period of unavailability have in reducing Staff confidence?

High □
Medium □
Low □
None □

FURTHER EXPLANATION

Section 3: IMPACT OF UNAVAILABILITY

Consider the effect on staff confidence that unavailability would cause, especially in those areas that may deal with customers or the general public.

Page 21 of 23

Phase 2 – Risk Assessment

- Required for FFIEC & NCUA compliance
- Identify threats to organization
  - Human Threats
  - Natural Threats
  - Technical Threats
- Estimate probabilities of identified threats occurring
- Assign critical ratings to identified risks
- Identify effective controls to reduce risks
- Make decisions on risk mitigation

Phase 3 – Recovery Strategies

- Develop strategies based on **BIA & Risk Assessment**
- Conduct a **Cost/Benefit Analysis**
  - What is the most **cost effective** strategy?
  - Invest $ in the **most effective** identified strategies
- The selected strategy(ies) should achieve:
  - A **controlled and effective response** to crisis situations
  - A **timely and cost effective** acquisition and utilization of resources
  - Recovery most **critical processes** in the shortest RTO

Phase 4 – Plan Development

- **Definition** - A previously established set of arrangements and procedures that enable an organization to respond to a disaster:

  Who, what, when & how

- **Scope of Project**
  - Cover the **worst case scenario** that is recoverable
  - Address **three areas** of exposure
    - Business service interruption
    - Financial loss
    - Legal responsibility
  - Address the **entire** financial institution

Plan Development Tasks

- Identify **Recovery Team Members**
- Develop **roles and responsibilities** for recovery team
- **Determine RTO's** for each functional area (based on BIA results)
- Develop **tasks and processes** for each business function
- **Assign** recovery tasks by Role
- Identify **resource requirements (**technology, equipment, vital records, vendors, etc.)
- Plan how the team will be **notified, mobilized and activated** in the event of a disruption

Phase 5 – Awareness & Training

- **Elements of Awareness & Training Programs:**
  - Policy Statement – Why is the plan being developed?
  - All components of the BCP
  - Who is involved and what are their roles
  - Where BCP information be found
  - How the BCP is activated

Awareness and Training is an ongoing program!!

Phase 6 – Maintenance & Testing

- Testing is required on an **Annual Basis** for compliance
- **What is testing?**
  - It is the technique of demonstrating the **correct operation of all equipment, procedures, processes and systems** that support the organization's infrastructure
  - The testing program has one overarching goal: ***the survivability of the organization***
- **Tests should focus on:**
  - Capabilities
  - Gaps and Shortcomings

Importance of Testing

- Enables efficient BCP **maintenance** through **early corrective action**
- Enables testing of many plan elements with **minimal cost and overall disruption**
- Provides **low-pressure atmosphere** that fosters learning
- Stimulates business continuity and **recovery preparedness** at all levels

Testing Methodology

- A **Four Phased** approach should be used to test BCP plans & components
  - **Test Planning**
  - **Test Execution**
  - **Post Test Review**
  - **Self-Assessment**
- Applying this method allows all tests to be **consistent**

Walkthrough Test

- Most **basic** type of test
- Source of the most **changes** to the plan
- Facilitated **discussion** of one or all recovery procedures
- Ensures members of recovery team are **familiar** with the the plan

Desktop Test

- **More involved** than Walkthrough – but still a discussion
- Specific **scenario** is applied to BCP
- Acts as both a **test & a training**
- Focuses on **demonstration** of knowledge
- **Role Playing** is key

Functional Test

- **Mobilization** of personnel at other sites
- Demonstration of **emergency management** capabilities
- Actual or simulated response to **alternate locations**
- Use of **actual communication** capabilities
- Varying degrees of **actuality**

Full-Scale Test

- Most **comprehensive**
- **Implements** all or portions of BCP
- Processing data and transactions using **back-up media**
- **Validation** of crisis response functions
- **On-the-scene** execution
- **Global participation** and interaction of internal and external management response teams

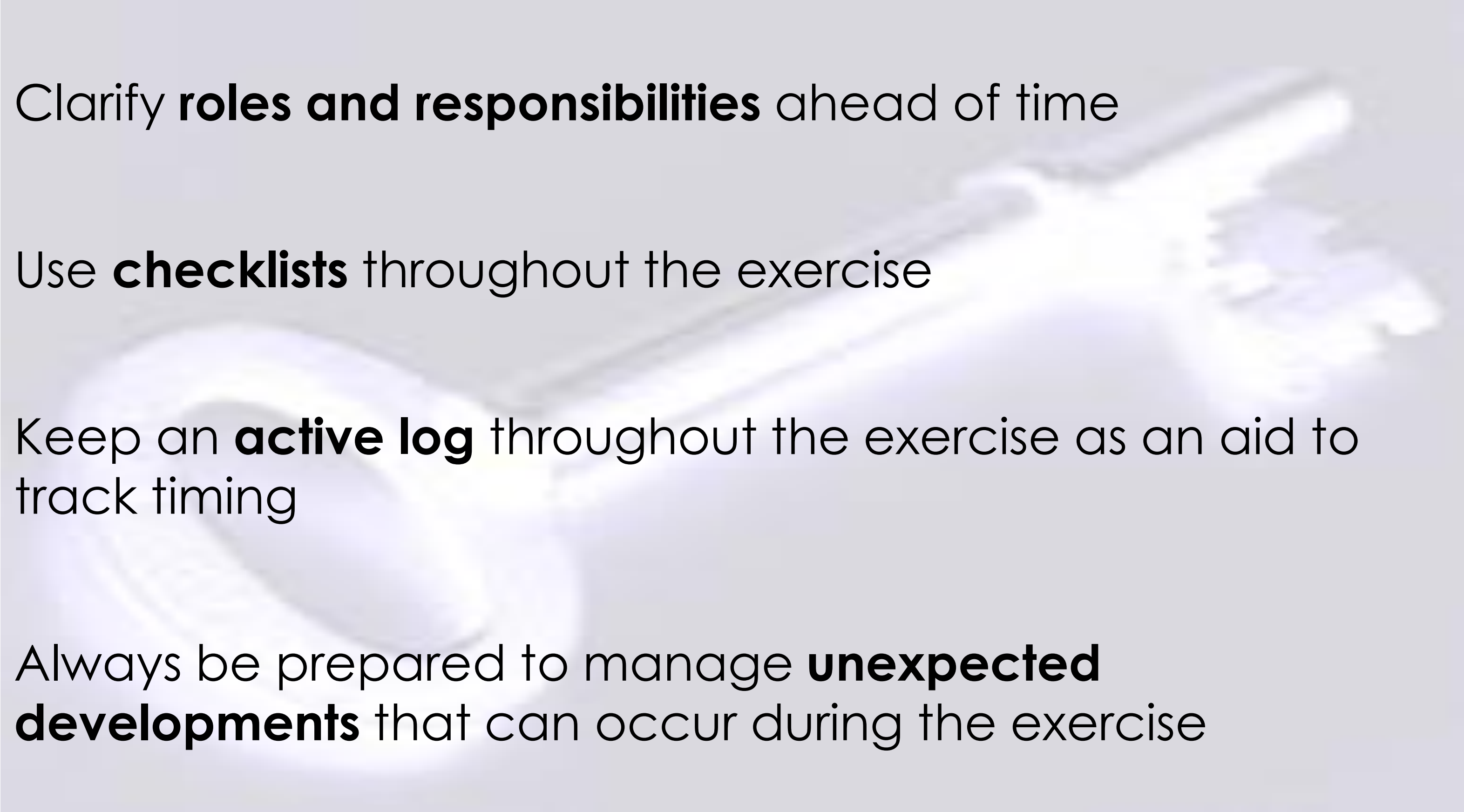
Test Frequency & Complexity

- BCP plans must be tested on an **annual basis**

- Frequency of **business unit** testing:
  - Based upon assigned **criticality** and **risk assessments**
  - Establish a **test schedule** to perform portion

- Complexity is based on the criticality of the **business function's processes**
  - This will determine how **robust** the test will be

Keys to Running a Smooth Exercise



Clarify **roles and responsibilities** ahead of time

Use **checklists** throughout the exercise

Keep an **active log** throughout the exercise as an aid to track timing

Always be prepared to manage **unexpected developments** that can occur during the exercise

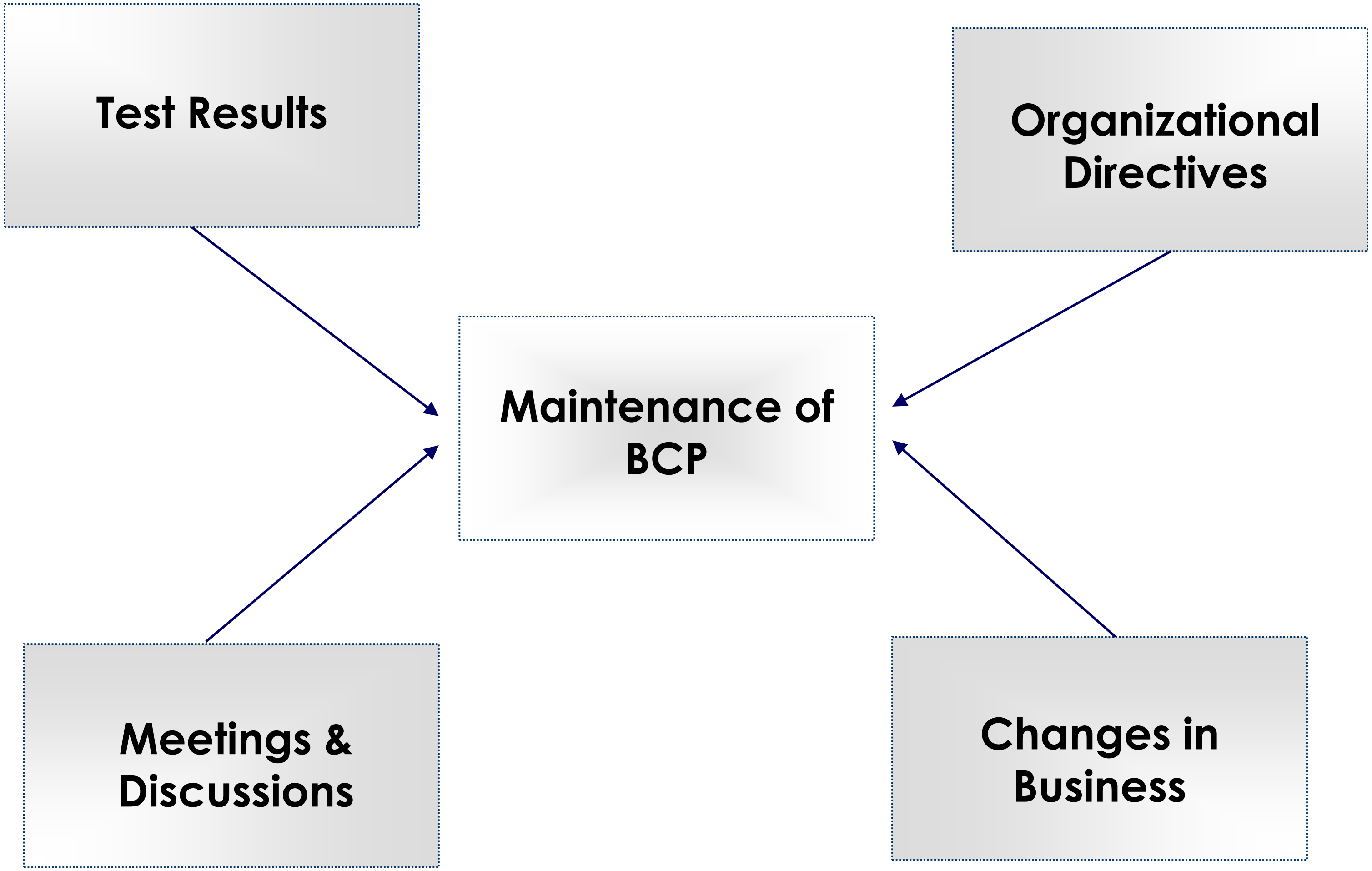
Questions for Analysis

- Can recovery of critical tasks be completed within the RTO?
  - If not, do alternate strategies exist?
- Was the scenario valid?
- Did the test effectively detail the activities to be completed during a disaster?
- Were the procedures clearly stated and understood?
- Is overall recovery possible using the current plan?

Plan Maintenance

- BCP is a “living” document
- Must change in conjunction with changes in the business activities it supports
- Development of a maintenance strategy to minimize the “gaps” between the plan and daily operations

Sources of Change



Test Results

Organizational Directives

Maintenance of BCP

Meetings & Discussions

Changes in Business

Lessons from Disasters

- **Airports and local transportation may be shut down**
  - Be prepared to recover without out-of-town personnel
  - Ensure you don’t test the same personnel in the same positions every time
- **Business Continuity tests become very valuable in real-world disruptions**
  - One company conducted 11 tests in 2004 and 2005. In one test, they learned that when a disaster strikes, they may not have access to cash to purchase critical supplies. Added in procedures to get money to disaster scene. That very lesson has proved critical in their ongoing recovery effort in Louisiana.

PLANet®

A Business Continuity Planning Tool for Financial Institutions

www.planetstrohl.com

STROHL SYSTEMS

Question & Answer Session