

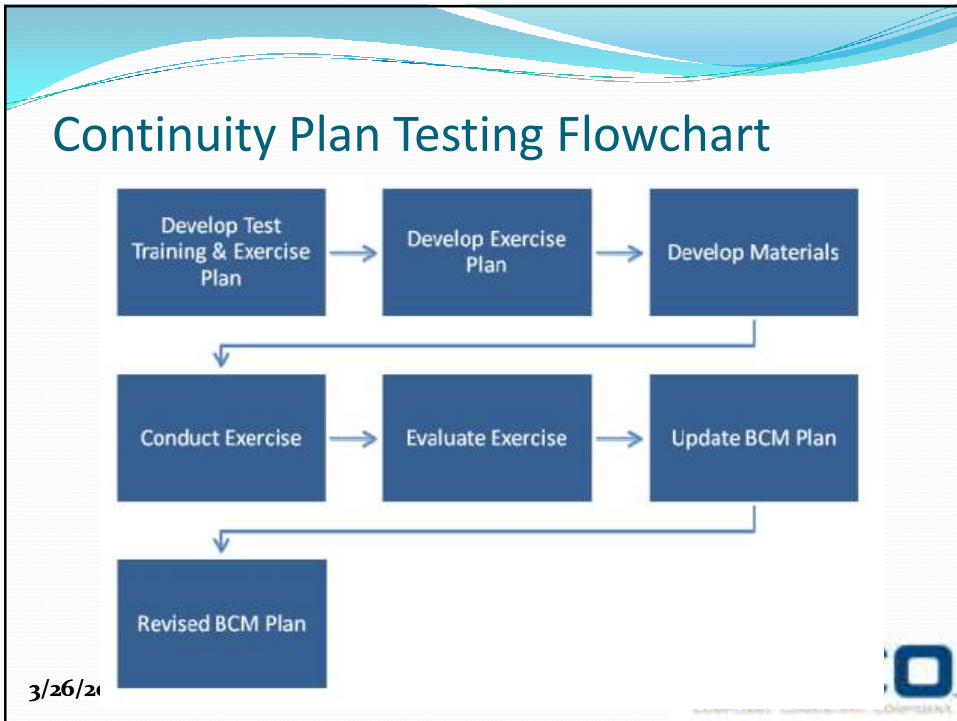

BEST
BANKERS EDUCATION SUPPORT AND TRAINING CENTER
NETWORKING AT THE BEST

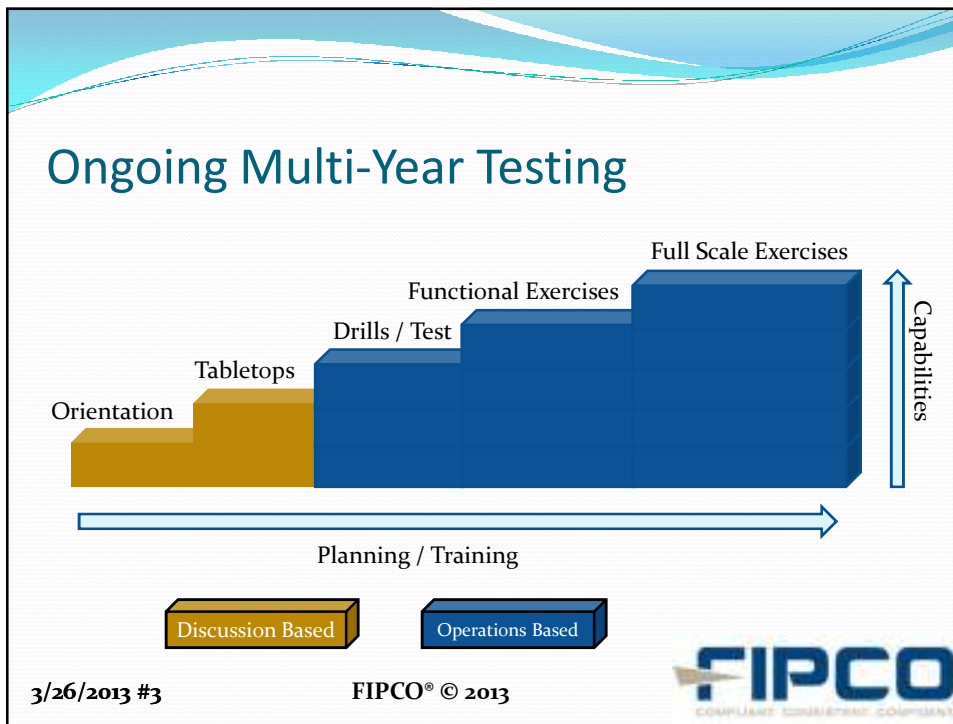
Surviving a Mock Disaster

Building an effective Tabletop Exercise

Presented by:
Ken M. Shaurette, CISSP, CISA, CISM, CRISC
FIPCO Director IT Services

3/26/2013 #1 FIPCO® © 2013





Types of Tests

Exercise Type	Description
Orientation	A seminar and/or briefing activity used to familiarize participants with BCM responsibilities
Test or Functional Drill	Coordinated, supervised activity normally used to test, develop, or maintain skills in a single operation or function in a single office or organization
Tabletop Exercise	Simulates emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing BCM plan and individual state of training and preparedness
Functional Exercise	Used to validate the capability of an organization to respond to a simulated emergency, in order to test one or more functions of the plan
Full Scale Exercise	Simulates an actual emergency; intended to evaluate operational BCM procedures and capabilities under simulated stressful conditions

Defining Roles and responsibilities

Position	Roles and Responsibilities
DR/BCP Coordinator / Information Security Officer	<ul style="list-style-type: none"> • Coordinate schedule / Exercise facilitator
Management Team	<ul style="list-style-type: none"> • Provide guidance and approval of Exercise Plan
IT - Manager / Network Admin	<ul style="list-style-type: none"> • Coordinate IT Recovery Plans • Plan and conduct IT Tests • Support BCP Coordinator in Development and exercising
Participants (all employees, DR/BCP Team, Business Area Managers/SME)	<ul style="list-style-type: none"> • Member of recovery team • Familiar with Plan • Know assignments • Perform specific business duties

3/26/2013 #5

FIPCO® © 2013



Functional and Full Scale Tests

- IT Recovery - test restore of technology, (i.e. data, network)
- Going offsite to a backup location tests recovery site preparedness, communications and utilities
- Trained and informed personnel are typically performing recovery steps
- Transaction testing verifies restore, connectivity and access using a person that knows the business process
- Community resources may be involved

What verifies the completeness of the Plan?

3/26/2013 #6

FIPCO® © 2013



Why Tabletop Exercises?

Provide a forum for the following:

- Team Building
- Validate the Plan Documentation
- Information Collection and Sharing
- Obtain consensus from team
- Evaluation of Differing Perspectives

3/26/2013 #7

FIPCO® © 2013



Why Tabletop Exercises?

Provide a forum for the following:

- Problem solving of complex issues
- Test considerations for new situations, ideas, processes and/or procedures
- Training/Awareness for management and staff

3/26/2013 #8

FIPCO® © 2013



Exercise Development Steps

Goals and Objectives –

What will success look like?

(SMART)

- Simple (concise)
- Measurable (how to document)
- Achievable (can this be done during the exercise?)
- Realistic (and challenging)
- Task Oriented (fits to business functions)

3/26/2013 #9

FIPCO® © 2013



Exercise Development Steps

Scope:

- Exercise Activities
- Departments Involved
- Hazard Type of Threat Source
- Geographic or outage Impact Area
- Staff Impacted
- Facilities Impacted

3/26/2013 #10

FIPCO® © 2013



Exercise Development Steps

Building a Scenario

- Choosing a Threat to Test
 - Vulnerability – Threat Assessment
- Start with simple basic scenarios – basic Fire minimal damage

Threat
Risk Asmt

Note: For example tornado incidents in the Midwest increased awareness of their threat risk.

The state may provide ongoing tasks of planning, preparing, and training for Tornado preparedness.

3/26/2013 #11

FIPCO® © 2013



Exercise Development Steps

Building a Scenario

- As your DR/BC matures - make scenarios more complex
- Consider the unexpected
- Don't share the full scenario before the event
- Does the DR/BCP Team always know when a tabletop will occur?

3/26/2013 #12

FIPCO® © 2013



Exercise Development Steps

Building a Scenario

- How quickly can you pull together key Business Team Members?
- How quickly can all key individuals be contacted and mobilized to the alternate location?
- Do you test the involvement of any outside parties? (i.e. law enforcement, safety, utilities, telephone, ISP)

3/26/2013 #13

FIPCO® © 2013



Exercise Development Steps

Objectives of Exercise

Tabletop Exercise Program Objectives

- To improve operational readiness by demonstrating knowledge of the DR/BCP Plan overall
- To improve bank-wide coordination and response capabilities for effective disaster response
- To identify communication pathways and problem areas between IT, outside entities (utilities, media) business areas, regional and state emergency operations centers
- To establish timely response for safety, recovery and restore to normal operation.

3/26/2013 #14

FIPCO® © 2013



Tips for an Effective Tabletop

- **Decide how much gloom and doom you want.**
 - Do you want this to be a physical event with assets damaged and destroyed,
 - Do you just want things inaccessible?
 - Do you want death and injuries, or just to test the ability to get work up and going someplace else?
 - How long will your downtime duration be?

3/26/2013 #15

FIPCO® © 2013



Conducting the Exercise

- **Set the Ground Rules**
 - Silence Cell Phones
 - Establish timelines – Maximum 4 Hours - breaks, lunch etc..
 - Who leads the exercise?
 - Consider issues that need to be tabled for later discussion

3/26/2013 #16

FIPCO® © 2013



Conducting the Exercise

- Set the Ground Rules
 - Accept the Scenario as Real
 - Stay in the Scenario - stay in the mindset that the disaster is really occurring
- Who will take notes – record issues / follow-up
 - Consider taping the exercise on an audio recorder

3/26/2013 #17

FIPCO® © 2013



Exercise – Evaluate - Update

- Planned Test scheduled in advance
 - Attendance by all BCP Team required
 - Team is aware of test scenario
- Document Team Member Attendance
- Confirm that all Team Members have their own up-to-date copy of the plan
- The BC coordinator confirms updates are in the plan.

3/26/2013 #18

FIPCO® © 2013



Exercise – Evaluate - Update

- Review policies and procedures
- Discuss business area changes since last updates?
- Confirm accuracy of phone numbers
- Verify Secure and accessible storage of plan (at home)
- Executive summary of the test and discussion results

3/26/2013 #19

FIPCO® © 2013



Resources

- NIST SP800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- Homeland Security Exercise and Evaluation Program (HSEEP) hseep.dhs.gov, FEMA: www.ready.gov/
- Michigan Emergency Partnership
www.michigan.gov/msp/0,4643,7-123-1593_3507_8920--,00.html
- CSOnline Business Continuity, www.csonline.com
- FIPCO, www.fipco.com/itservices

TIP

Experience has shown that well planned and interesting exercises yield a high level of preparedness with personnel who are able to better cope with the stressful environment of an actual emergency.

3/26/2013 #20



Sample Tabletop Exercise Testing Fire in the Server Room (a/k/a Data Center)

[CLICK
HERE](#)


3/26/2013 #21

FIPCO® © 2013



Bank
Business Continuity Tabletop Exercise
Threat = Fire in Server Room
DATE, 2013

Facilitated By:
Ken M. Shaurette, CISSP, CISA, CISM, CRISC
FIPCO Director IT Services



FIPCO © 2013
1

Today's Agenda

- Structure of Today's Discussion
 - Set Objectives
 - General overview of DR/BCP
- Exercise Assumptions
- Scenarios
 - Discussions
- Lessons Learned
- Next Steps

Anyone have concerns with recording today's exercise?




FIPCO © 2013
2

Schedule

• Introductions	10:00 – 10:10
• Business Continuity Overview & Plan Review / Assumptions	10:10 – 10:30
• Exercise	10:30 – 12:00
• Lunch	12:00 – 12:30
• Exercise	12:30 – 01:30
• Feedback & Wrap-up	01:30 – 02:00

Moderator: Ken M. Shaurette




FIPCO © 2013
3

Exercise Assumptions

(Note: cell phones off or on mute)

- Scenario Setup
 - Based on a fire in or near the server area at the main facility
 - Everyone is working on the day of the fire
- During each scenario slide we must stay in the mindset that the disaster is really occurring – You're not discussing what you would do, you will be discussing what you are doing!
- FIPCO team is the moderator for the day
- Bank team will hold discussions during each scenario slide, FIPCO team cannot provide advice but can answer questions related to the scenario



FIPCO © 2013
4

Goals & Objectives

- Educate teams & validate Business Continuity Plan content under a fire event disaster scenario
- Provide practice and Confidence
- Ensure each members plan is up to date
- Demonstrate knowledge of :
 - Evacuation process.
 - Disaster declaration process.
 - Business resumption, IT recovery.
- Identify and Report on Improvement Recommendations
- Meet Compliance Initiatives

FIPCO

FIPCO © 2013 5

Purpose of the Continuity Plan

- Ensure controlled emergency response.
- Minimize the impact of the event.
- Direct and assist employees' response to the event.
- Provide Documentation and Knowledge
- Identify and document mission-critical activities and the staff and resources needed to resume those activities.
- Resume operational capability
- Get Bank back to normal

FIPCO

FIPCO © 2013 6

Business Continuity Lifecycle

Recovery & restoration

- ✓ Long-term continuity
- ✓ Repair/replace
- ✓ Migration
- ✓ Resume "normal" service

Response

- ✓ Recognition & Assessment
- ✓ Escalation & Notifications
- ✓ Declaration of Disaster

Resumption

- ✓ Initial
- ✓ Short-term continuity
- ✓ Critical Business Activities Resumed

FIPCO

FIPCO © 2013 7

Recovery Plan Components

- Functional Testing Schedule
- Business Impact Analysis – Recovery Times
- Threat Risk Matrix – prioritized threats
- Employee Phone Chain
- Recovery Procedures
- Vendor List
- Emergency Contact List (Media, Security, Safety)

FIPCO

FIPCO © 2013 8

Exercise Instructions

- Participant Open Discussion
- Use Business Continuity Plan and related materials as your resources
- No Wrong Answers
- The scenario is that a fire occurs in the data center. Slides will communicate stages of the disaster.
- Bank team will discuss how you will handle each of the scenarios
- Reminder - Once in we're in scenario slides the discussions should be on your actual processes and not be trying to figure out the processes
- After each scenario slide we have a discussion to determine if you covered everything that is necessary to recover
- FIPCO is recording today's exercise so that we can review how you responded and analyze today's results so that we can provide guidance for improvement



Scenario: Incident & Evacuation

- **2pm Monday:**
 - A fire starts in the main data center facility
 - Flames and smoke are noticed by an employee
 - There are 6 customers in various areas of the building
 - Everyone on the staff is working



Discussion

- What is the process if someone notices a fire?
- How is the evacuation notification spread throughout the bank?
- What actions do the staff take before evacuating?
- How / Who evacuates guests/customers in the building?
- Where is the rendezvous location?
- What activities are performed at the rendezvous location?
 - Who is in charge?
 - What is communicated to the employees?
 - How do you account for missing employees?
 - Who do you report your departments' status to?
 - What is the policy for staying / leaving?



Scenario: Damage Assessment

- **2:30pm Monday**
 - Evacuation was successful
 - The fire has damaged the facility
 - Everything in the data center is destroyed
 - It is determined that no one can re-enter the facility



Discussion

- Who determines if it is safe to re-enter the building or not?
- Who's responsible for the Damage Assessment process? How does each department contribute?
- As management, who do you notify and how?
 - Is there communication to the other branches? Who is responsible for this?
 - What message do you give to your employees regarding inquiries (customer, press etc.)?
 - Where do you call from? How are phone services affected?
 - Who else would you call?

FIPCO © 2013

13



Scenario: Disaster Declaration

- **6pm Monday**
 - Damage Assessment has been completed and the bank has extensive damage
 - ✦ The IT department has the most damage and recovery is necessary at the identified recovery location.
 - ✦ All IT services provided from the bank are impacted.
 - ✦ The bank requires clean-up and this process will take at least one week.

FIPCO © 2013

14



Discussion

- Was a disaster declared?
- Who has the responsibility to declare a disaster?
- Who is on the Disaster Recovery / Crisis Management Team?
- How is security of the building handled?
- What is the process for closing the office?
- Where does staff resume working?
- Who / What is the process for salvaging bank assets?

FIPCO © 2013

15



Scenario: Disaster Response

- **7 pm Monday**
 - A disaster has been declared
 - ✦ The Disaster Recovery / Crisis Management Team has created a Command Center at the alternate location

FIPCO © 2013

16



Discussion

- Who activates the Call Tree? What is the message to teams? What if you can't get hold of someone in the Call Tree?
- Once you receive the disaster declaration message, what is your response?
 - Where will you redirect your customer to?
 - What critical records are in the damaged facility?
 - How can you verify the status of that days transactions?
 - How are lost transactions handled?
 - What services are / are not impacted?
- Does the Main Office or branch location(s) open on Tuesday?



Scenario: Resumption

- 8am Tuesday
 - IT is working on recovering critical resources. Current Status:
 - No Internet.
 - No Access to IT Resources.
 - Phones working in 'remote survivability' mode.
 - Main Office is open for business in alternate location.



Discussion

- What is the message to customers?
- Are your manual procedures documented? What do you do?
- What is the status of recovery for the core banking system / IT infrastructure?
- How do you communicate to the Crisis Mgmt Team? How does Crisis Mgmt Team communicate to other teams?



Scenario: Recovery

- 8am Wednesday
- IT has recovered parts of the infrastructure but it is up with limited access – most critical parts.
- Recovery of systems continues



Discussion

- What is IT recovering now?
- Without access to systems, what do you do?
 - Do lost transactions need to be input?
 - What is the order of posting lost transactions?
 - How do you catch up on manual work already processed?

Scenario: Alternate Site is Up

- 8am Thursday
- IT has recovered critical systems at the alternate site.
- Non-critical systems are not up yet such as:
 - > ?
 - > ?
 - > ?
- Branch(es) open for business.

Discussion

- With access to additional systems, what do you do?
 - Are there additional lost transactions need to be input?
 - How do you catch up on manual work already processed?

Lessons Learned

- Review follow-up information that should be included in the plan.
- Review major learning opportunities.
- Highlights of exercise.
- Recommendations for future exercises.

Next Steps / Action Items

- FIPCO Analysis
- Executive Summary
- Recommendations
- Management Actions
- Post Mortem Narrative

Thank you
Ken M. Shaurette
FIPCO Director IT Services
Phone: (608) 441-1251

