Surviving a Mock Disaster
Building an effective Tabletop Exercise

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

Continuity Plan Testing Flowchart
Ongoing Multi-Year Testing

Orientation

Tabletops

Drills / Test

Functional Exercises

Full Scale Exercises

Planning / Training

Capabilities

Discussion Based

Operations Based

Types of Tests

<table>
<thead>
<tr>
<th>Exercise Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orientation</td>
<td>A seminar and/or briefing activity used to familiarize participants with BCM responsibilities</td>
</tr>
<tr>
<td>Test or Functional Drill</td>
<td>Coordinated, supervised activity normally used to test, develop, or maintain skills in a single operation or function in a single office or organization</td>
</tr>
<tr>
<td>Tabletop Exercise</td>
<td>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</td>
</tr>
<tr>
<td>Functional Exercise</td>
<td>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</td>
</tr>
<tr>
<td>Combination Test</td>
<td></td>
</tr>
<tr>
<td>Full Scale Exercise</td>
<td>Simulates an actual emergency; intended to evaluate operational BCM procedures and capabilities under simulated stressful conditions</td>
</tr>
<tr>
<td>ALL OUT TEST</td>
<td></td>
</tr>
</tbody>
</table>
Defining Roles and responsibilities

<table>
<thead>
<tr>
<th>Position</th>
<th>Roles and Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR/BCP Coordinator / Information Security Officer</td>
<td>• Coordinate schedule / Exercise facilitator</td>
</tr>
<tr>
<td>Management Team</td>
<td>• Provide guidance and approval of Exercise Plan</td>
</tr>
<tr>
<td>IT – Manager / Network Admin</td>
<td>• Coordinate IT Recovery Plans</td>
</tr>
<tr>
<td></td>
<td>• Plan and conduct IT Tests</td>
</tr>
<tr>
<td></td>
<td>• Support BCP Coordinator in Development and exercising</td>
</tr>
<tr>
<td>Participants (all employees, DR/BCP Team, Business Area Managers/SME)</td>
<td>• Member of recovery team</td>
</tr>
<tr>
<td></td>
<td>• Familiar with Plan</td>
</tr>
<tr>
<td></td>
<td>• Know assignments</td>
</tr>
<tr>
<td></td>
<td>• Perform specific business duties</td>
</tr>
</tbody>
</table>

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?
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

Why Tabletop Exercises?

Provide a forum for the following:

- Check that functional testing occurs
- Problem solving of complex issues
- Test considerations for new situations, ideas, processes and/or procedures
- Training/Awareness for management and staff
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)

Exercise Development Steps

Scope:

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

Building a Scenario

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

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.

Threat Risk Assessment

<table>
<thead>
<tr>
<th>Threat Description</th>
<th>High Risk</th>
<th>Medium Risk</th>
<th>Low Risk</th>
<th>Risk Ratings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidental-explosion—off-site</td>
<td>★★</td>
<td>★</td>
<td>★</td>
<td>★★</td>
</tr>
<tr>
<td>Accidental-explosion—on-site</td>
<td>★★</td>
<td>★</td>
<td>★</td>
<td>★★</td>
</tr>
<tr>
<td>Aircraft-crash</td>
<td>★★</td>
<td>★</td>
<td>★</td>
<td>★★</td>
</tr>
<tr>
<td>Ancillary-equipment-failure</td>
<td>★★</td>
<td>★</td>
<td>★</td>
<td>★★</td>
</tr>
<tr>
<td>Arson</td>
<td>★★</td>
<td>★</td>
<td>★</td>
<td>★★</td>
</tr>
<tr>
<td>Bomb-threat</td>
<td>★★</td>
<td>★</td>
<td>★</td>
<td>★★</td>
</tr>
<tr>
<td>Bombing</td>
<td>★★</td>
<td>★</td>
<td>★</td>
<td>★★</td>
</tr>
<tr>
<td>Central-computer-equipment-failure</td>
<td>★★</td>
<td>★</td>
<td>★</td>
<td>★★</td>
</tr>
<tr>
<td>Computer-Intruder</td>
<td>★★</td>
<td>★</td>
<td>★</td>
<td>★★</td>
</tr>
</tbody>
</table>
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?

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)
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.

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?
  - Do you test unavailable key people?
  - How long will your downtime duration be?
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

Conducting the Exercise (cont...)

- 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
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.

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
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.

Resources

- NIST SP800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- Wisconsin Emergency Management emergencymanagement.wi.gov/
- CSOonline Business Continuity, www.csoonline.com
- FIPCO, www.fipco.com/itservices
If Time Allows, if not email kshaurette@fipco.com

Sample Tabletop Exercise Testing

FIRE
CLICK HERE

STORM
CLICK HERE