Creating Realistic Continuity Exercises Using Simulation Cells

John A. Jackson FBCI (hon), CORE Executive Vice President Fusion Risk Management, Inc. June 18, 2013 – Session B3

Topics to Discuss Today

- Exercises and Drills – The Options
- Multi-Plan Tabletops
- Regional Interdependencies
- Simulation Cell Integration
- Wrap-up
Plan the Test vs. Test the Plan

- In my opinion, most organizations focus too much effort on Planning a Test
- Conversely, too often the actual plans are NOT tested during a test
- Let’s reflect on how most organizations plan for a test
- Organizations should advocate more realistic testing to identify problems which can be addressed before an incident occurs

Exercise Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Approach</th>
<th>Duration</th>
<th>Benefit</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Review (Orientation)</td>
<td>Plans are reviewed individually or in a group in a group setting. Plan reviewers are asked about their experience. Plans are evaluated for gaps and weaknesses. Gaps are identified and corrective actions are defined.</td>
<td>Individual review similar to an open book test. Could be executed in flow survey. Monkey.</td>
<td>1–2 hours</td>
<td>Content validation awareness. Identify, assess, and address improvement areas. Ensure plans are complete, accurate, and define all necessary procedures.</td>
<td>Does not verify effectiveness. Does not test communications. Does not validate Contingency &amp; Control of plan activities.</td>
</tr>
<tr>
<td>Single-team (Orientation)</td>
<td>Plans can be reviewed individually or in a group in a group setting. Plan reviewers are asked about their experience. Plans are evaluated for gaps and weaknesses. Gaps are identified and corrective actions are defined.</td>
<td>Group facilitated</td>
<td>2–3 hours</td>
<td>Identify, assess, and address improvement areas. Ensure plans are complete, accurate, and define all necessary procedures.</td>
<td>Does not verify effectiveness. Does not test communications. Does not validate Contingency &amp; Control of plan activities.</td>
</tr>
<tr>
<td>Multi-team (Orientation)</td>
<td>Multi-team discussions are facilitated to gain an understanding of team interactions and communications. Leaders to develop assumptions during multi-team discussions are facilitated.</td>
<td>Group facilitated</td>
<td>2–4 hours</td>
<td>Identify, assess, and address improvement areas. Ensure plans are complete, accurate, and define all necessary procedures.</td>
<td>Does not verify effectiveness. Does not test communications. Does not validate Contingency &amp; Control of plan activities.</td>
</tr>
<tr>
<td>Structured Walkthrough (Advanced)</td>
<td>Scenario-based Tabletop Review with specific questions about the ability of the team to respond to the given situation.</td>
<td>Group facilitated Scenarios variables are introduced</td>
<td>3–4 hours</td>
<td>Evaluate decision-making processes. Ensure actions are accurately described in Plan.</td>
<td>Limited in proving response capabilities.</td>
</tr>
</tbody>
</table>
# Exercise Types - 2

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Approach</th>
<th>Duration</th>
<th>Benefit</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation</td>
<td>Planned</td>
<td>• Participants are placed into a situation based upon a disaster scenario and expected outcomes upon the plan. Participants are forewarned, giving plan owners and participants time to review the plans.</td>
<td>1–6 hours</td>
<td>• Provides ability to evaluate the effectiveness of the people, process and tools. Good practice session.</td>
<td>• Does not validate alternate facilities/processes.</td>
</tr>
<tr>
<td></td>
<td>Unplanned</td>
<td></td>
<td>6–24 hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Parallel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Planned</td>
<td>• Participants are “surprised” giving plan owners and participants time to review the plans.</td>
<td>6–24 hours</td>
<td>• Ensures high-level of reliability without interrupting normal operations.</td>
<td>• Expensive, involves significant resources.</td>
</tr>
<tr>
<td></td>
<td>Unplanned</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Interruption</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Planned</td>
<td>• Disaster is replicated to the point of ceasing normal operations. All business is conducted using alternate facilities/processes.</td>
<td>6–24 hours</td>
<td>• Demonstrates a high degree of program maturity. Most reliable test of BCP.</td>
<td>• Potentially introduces a real disaster.</td>
</tr>
<tr>
<td></td>
<td>Unplanned</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Testing the Entire Recovery Process

![Testing the Entire Recovery Process Diagram](image-url)
MULTI-PLAN TABLETOPS

Multi Plan Tabletops

- One of the most often overlooked aspects of Business Continuity Planning is a plan’s reliance upon or interaction with other BCP plans
- Think about who relies on you and who you rely upon
- Test the ability of individual plans to respond to the scenario
- Allows you to observe the testing of other plans that may interface with or affect your own plans
- Determine your plans’ awareness of and interface to company Emergency Response Plans, Crisis Management Plans and Contingency Procedures
- Identify plan interface concerns and identify subsequent remediation tasks
Set Clear Objectives

- Conduct a mini review of your plans (by individual plan owner) prior to the tabletop to improve familiarity and identify high level issues
- Test the ability of individual plans to respond to the scenario through all four stages of Recovery (Respond, Recover, Restore, Resume)
- Ensure that if a plan does not cover some aspect that the plan owner knows how that would be addressed (other plan or other team) i.e. do you know who is doing what if your plan doesn’t cover an issue
- Allow plan owners to observe the testing of other plans that may interface with or affect your own plans
- Determine a plans’ awareness of and interface with Company Emergency Plans, Crisis Response Plans and Contingency Procedures
- Identify changes, additions or deletions to each individual plan
- Identify plan interface concerns and identify subsequent remediation tasks

Create and Adhere to a Time Line

- 09:00 - Start and Introduction – 10 minutes
- 09:10 – Complete Assessment Document– 10 minutes
- 09:20 - Plan Review – 45 minutes
- 10:05 – Break – 10 minutes
- 10:15 – Response – 20 minutes
- 10:35 – Recovery – 25 minutes
- 11:00 – Restoration – 25 minutes
- 11:25 – Break – 10 minutes
- 11:35 – Resumption – 25 minutes
- 12:00 - Post Mortem – 25 minutes
- 12:25 – Questions – 15 minutes
- 12:40 – Complete Evaluation and “Post Mortem” assessment – 20 minutes
- 13:00 - Close
Regional Inter-Dependency Workshops

- A concept I have advocated for years is an exercise called a Regional Inter-Dependency Workshop
- The concept is to identify external organizations that could impact your recovery
- Whether you do this or not, the concepts are something you should think about
The Interdependency Workshop

The workshop is designed to assist an organization in understanding:

- The risks you face based on your geographic location
- The Plan’s interdependencies with the local public agencies and the infrastructures they provide
- The effect of a public infrastructure failure or outage on firms in a given geographic area
- The business to business interdependencies that exist
- How the interdependencies would further complicate, and possibly delay individual companies recovery efforts

Interdependency Exercise Steps

- Define a scenario
- Consider the geographic area
- Identify the Public Agency impacts
- Identify the potential business interactions
- Discuss the scenario and the interdependencies that might occur
Defining a Scenario

- The infrastructure disruption under consideration may be due to a natural disaster (e.g. flood, tornado, ice storm, snow storm, etc.) or a man-made event (e.g., regional power outage, terrorism).
- The disruption might affect a single infrastructure (e.g. electric, telecommunications, water, etc.), or a single building (e.g. fire, anthrax contamination) in the defined area of the city.
- Whatever it is, make it realistic and believable!

A Regional Event In Chicago

Categories of Interdependencies to consider?

- Major Businesses
- Government Offices
- Utilities
- Medical Facilities
- Transportation
- Public Areas
What to Know About Other Businesses

- Why is there an interdependency concern?
- What is their overall recovery strategy?
  - What is covered?
  - What is not covered and why not?
- Recovery Time Objective by shared Application (time to recover and make operational)
- Recovery vendor and primary site if using a shared vendor
- Major business to business interface points, systems, data feeds
- Contact points during a disaster, and how to contact
- Major concerns about their recoverability

SIMULATION CELLS – HOW TO PLAN, HOW TO USE
Simulation Cells

- Most tests do not include the realistic aspect of having some participants “act” as external parties, such as concerned citizens or neighbors, media, emergency management personnel or other constituencies.
- Creating a Simulation Cell with scripted injects, called or texted in to the command center, can increase the “reality” of a test or exercise.

First Step – Do The Planning
Create a Set of Objectives

- **Major Exercise Objective:**
  - Drill the response to a major incident at the XYZ site, their handling of a significant number of casualties and fatalities, and their interaction with the Corporate Crisis Team.

- **Key Objectives:**
  - Exercise several new Team members
  - Test the ability to launch the XYZ notification tool
  - Establish and exercise Team interactions
  - Observe the Teams’ ability to respond to and manage injuries and casualties
  - Determine the adequacy of Emergency Plans, Crisis Response Plans and Contingency Procedures and observe the degree to which they are actually utilized
  - Test the Teams’ responsiveness to external agencies or entities who become involved
  - Observe any responses to any Regulatory issues that might arise

Develop a Scenario

- **Scenario – High Level**
  - A small plane (company jet, 12 seat or so) crashing into the point where the Production Building and the Quality Control buildings meet
  - Plane is taking off from the airport, and due to the heat and a lack of lift, crashes into the two buildings.
  - The Airport is on direct flight path to airport and high heat temperatures would be a contributing factor – real life situation
Identify Impacts

- Major impacts include:
  - Evacuations
  - Damage to buildings
  - Ruptured water and gas lines
  - Injuries and 1 fatality
  - Some fire as a result of jet fuel
  - Concerns of schools, hospitals, neighbors – all adjacent areas
  - Involvement of the NTSB and local airport authorities
  - Production impact from damage to the manufacturing building and compromising of product quality
  - Potential impact to use of the plant during investigation

Create a Story Line

- Story Line Components
  - The following points will be considered for inclusion into the script:
    - Summer day, high temp, no rain, no fog, excessive heat causes plane to drop – short runway – airplanes regularly have issues in high temp periods
    - Plane hits Production and QC buildings
    - Local alarm (continuous) (Bldg.) or General alarm (site) (intermittent), evacuate all buildings, go to rally points
    - Emergency team responds
    - Contact fire and police
    - Emergency team members check buildings to ensure evacuations, within limits of what they can do (no Medical Team, no Fire Equipment)
    - Emergency Team calls Incident Commander
    - IC responds to the site of the impact
    - IC calls into Command Center
    - Crisis Team Convenes
    - Airport contacts plant security to confirm plane crash and location of crash
    - Fire occurs – boxes for packaging, some gases, fuel from plane
Decide on the Simulators

- Simulators are simply people acting out a role in the exercise
- They may represent:
  - Media
  - Police, Fire or Emergency Management
  - Concerned 3rd Parties
  - Shareholders, Regulators
  - Others are defined by the Story Line
- The more they know about the role they are playing, the better
- The more they “adopt” their role, the better

Define an Evaluation Process

- **Evaluation Process**
  - Use an observation and evaluation process where all numbered objectives are equally weighted.
  - Objectives could be measured and evaluated according to the following scale:
    - Score of 3 - The Process or Practice worked effectively, with no observed issues or omissions
    - Score of 2 - The Process or Practice worked reasonable effectively, with noted minor issues
    - Score of 1 - The Process or Practice was used or attempted, but had significant issues or omissions
    - Score of 0 - The Process or Practice did not exist or was not utilized
Create a Minute by Minute Script

Next Step – Kick off the Exercise
Drill Overview - Description

- **Description of Incident**
  - You are in your offices. On the site, it is break time. Most employees are in the cafeteria.
  - A very loud noise is heard (airplane engines), approaching the site.
  - A loud crash occurs. Alarms are sounding.
  - A small jet plane has crashed into the roofs of the Quality Control and Production buildings.
  - There is an explosion and fire. A plane is visible on the roof and partially into the Production building.

Drill Overview - Facts

- **Facts to Consider - Summary**
  - Facts as known are as follows:
    - Plane appears to be a small corporate jet
    - Impact damages roofs, an explosion is heard, fire is apparent
    - The plane is visible on the roof, partially into the Production building
    - Injuries and any fatalities are unknown at this time
    - Debris field is 100 yards around the plane
    - Weather conditions are unusually warm, 98 degrees Fahrenheit, light wind, dry and sunny
Diagrams Help!!

Point of Impact

As Do Pictures from the Site
Drive the Simulation Cell’s Involvement through Message Sheets

CONFIDENTIAL DRILL MESSAGE

DELIVERY METHOD: Phone call to number
XXX-XXXX-xxxx

TYPE: MS
DATE: MAY-09-2013

CONTROL #: 2
TIME: T+0:02

SIM CELL ASSIGNMENT: Sim Cell Person A

FOR: Person A - Incident Commander

FROM: Emergency Team Leader

MESSAGE:
**THIS IS A DRILL**
This is the Emergency Team Leader - Based on the situation, I am confident we will have a number of casualties, we better get some ambulances here as soon as possible - please update us when you can

**THIS IS A DRILL**

Supporting information or additional references: Initial casualty report

CONTROLLER/SIMULATOR INSTRUCTION:
This text provides guidance as to how the controller or Sim Cell team will administer this message:
Await response and document on message sheet, Leave voice message and request call back if no immediate answer, track call back on message sheet
CONFIDENTIAL DRILL MESSAGE

DELIVERY METHOD: Phone call to number xxx-xxx-xxxx
TYPE: MS DATE: MAY-09-2013
CONTROL #: 3 TIME: T+003
SIM CELL ASSIGNMENT: Sim Cell Person B

FOR: Plant Manager - Sr Mgr. and Chief Emergency Officer

FROM: Incident Commander

MESSAGE: **THIS IS A DRILL**
CONDITIONAL INJECT
We have a serious incident at the plant involving a plane crash, please assemble the MST at the EOC

**THIS IS A DRILL**

Supporting information or additional references: MST notified to assemble

CONTROLLER/SIMULATOR INSTRUCTION:
This text provides guidance as to how the controller or Sim Cell team will administer this message:
If either xxxxx or xxxxx have not activated the MST members, then xxxxxx will need to prompt them to do the activation

---

CONFIDENTIAL DRILL MESSAGE

DELIVERY METHOD: Phone call to number xxx-xxx-xxxx
TYPE: MS DATE: MAY-09-2013
CONTROL #: 6 TIME: T+006
SIM CELL ASSIGNMENT: Sim Cell Person A

FOR: Person C - Communications Manager

FROM: Gatehouse Security

MESSAGE: **THIS IS A DRILL**
This is the Gatehouse, we are starting to receive a number of employee, media and concerned outside party calls about the smoke and don't know how to respond to them. What do you want us to do with the calls coming in?

**THIS IS A DRILL**

Supporting information or additional references: Gatehouse needs phone relief

CONTROLLER/SIMULATOR INSTRUCTION:
This text provides guidance as to how the controller or Sim Cell team will administer this message:
Await response and document on message sheet. Leave voice message and request call back if no immediate answer, track call back on message sheet
CONFIDENTIAL DRILL MESSAGE

DELIVERY METHOD: 2 way Radio
TYPE: MS
DATE: MAY-09-2013
CONTROL #: 7
TIME: T+007
SIM CELL ASSIGNMENT: Sim Cell Person C

FOR: Person D - General Manager
FROM: Emergency Team Leader

MESSAGE: **THIS IS A DRILL**
xxx, xxxxx xxxxxx at the local airport has called the main site phone number asking if we can you confirm a crash at the site and provide them any additional information? He said they are trying to get a manifest for the flight but they believe this was a passenger flight only. Do you want to call him back or should I?

**THIS IS A DRILL**

Supporting information or additional references: Airport contacts

CONTROLLER/SIMULATOR INSTRUCTION:
This text provides guidance as to how the controller or Sim Cell team will administer this message:
Await response and document on message sheet. Leave voice message and request call back if no immediate answer, track call back on message sheet.

Last Step – What Did We Learn
**Post Mortem Review**

- The purpose of a Post Mortem Review is to identify the effectiveness of our Continuity Plan capabilities and to identify lessons learned to enhance the plan.
- Specifically, we will:
  - Discuss the decisions that were made and the impacts on continuity of operations during a Facility outage
  - Analyze the effectiveness of the plan
  - Identify areas for improvement
  - Plan Interactions

Let’s discuss how things went!!

**Score Specific Aspects of the Drill**

- **Crisis Communications:**
  - Observe the effectiveness of the Crisis Communications process for:
    - Responding to media inquiries
      - Score ____:
    - Dispatching and/or coordinating onsite spokespersons
      - Score ____:
  - Observe and comment on the effectiveness of the process for how communications personnel at Corporate will:
    - Coordinate public/media relations
      - Score ____:
    - Share responsibilities
      - Score ____:
  - Ensure consistent messages to the full range of internal and external stakeholders
    - Score ____:
Discuss the Exercise Process

- Was this a useful exercise for you, why?
- What do you think went especially well?
- What did not work well, and why?
- Were there any aspects of the exercise that were confusing or ambiguous?
- Did the exercise flow in a manner that you believe represented an actual incident response?

Discuss Lessons Learned

- Were there any surprises that came up during the exercise?
- What lessons did you learn and what should be done as a result?
- What would make a next exercise more valuable to you or the team?
Take-Aways from this Morning’s Discussion

- Drills and Exercises come in all shapes and sizes
- Expanding plan exercises to address internal and external interfaces helps to broaden people’s perspectives
- Using Simulation Cells adds realism and forces a time schedule that most tests never address
- The more realistic the exercise, the better the value

Creating Realistic Continuity Exercises Using Simulation Cells

John A. Jackson FBCI (hon), CORE
Executive Vice President
Fusion Risk Management, Inc.
June 18, 2013 – Session B3