Business Continuity Tabletop Exercise FIRE

By Ken M. Shaurette, CISSP, CISA, CISM, CRISC

FIPCO Director IT Services

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Today's Agenda

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

Schedule

Introductions
Business Continuity Overview & Plan Review
Exercise
Feedback & Wrap-up

Moderator: Ken M. Shaurette

Exercise Assumptions

- Scenario Setup
  - Based on a fire in the data center
  - Everyone is working on the day of the fire
- During scenario slides we must stay in the mindset that the disaster is really occurring during each scenario slide – 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

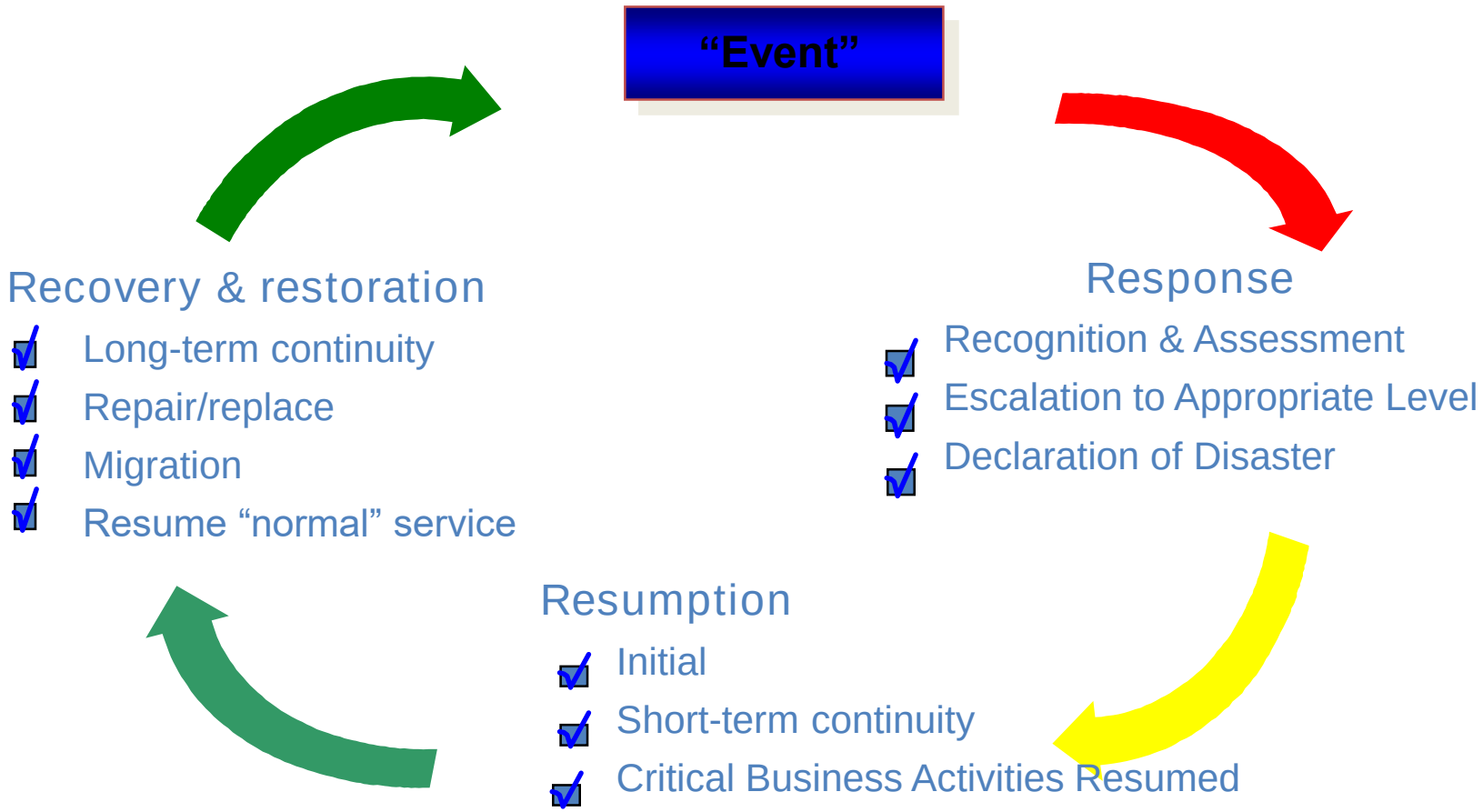
Goals & Objectives:

- Educate teams & validate Business Continuity Plan content under a fire event disaster scenario
- Demonstrate knowledge of :
  - Evacuation process.
  - Disaster declaration process.
  - Business resumption, IT recovery.
- Identify and Report on Improvement Recommendations
- Meet Compliance Initiatives

Purpose of the Continuity Plan

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

Business Continuity Cycle



Your Recovery Plan Components

- Functional Testing Schedule
- Recovery Matrix
- Employee Phone Chain
- Recovery Procedures
- Vendor List

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
  - The are 10 customers in 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 inquires (customer, press etc.)?
  - Where do you call from? How are phone services affected?
  - Who else would you call?

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.

Discussion

- Was a disaster declared?
- Who has the responsibility to declare a disaster?
- Who is on the 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?

Scenario: Disaster Response

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

Discussion

- Who activates the Call Tree? What is the message to teams? What if you can't get a 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 other <<<< Bank >>>> branch location 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.
    - <<<< Bank >>>> branch is open for business.

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 the teams?

Scenario: Recovery

- 8am Wednesday
- IT has recovered parts of the infrastructure but it is up with limited access.

Discussion

- What is IT recovering now?
- With 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 is 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.
- Debris from building sitting in the parking lot partially burned, who is in charge of going through it to make sure there isn't confidential information there, pc's that are partially burned who is in charge of determining if the hard drives still need to be forensically swiped instead of just letting fire department haul it all away to the dump or landfill where it could be stolen

Lessons Learned

- Debris from building sitting in the parking lot partially burned, who is in charge of going through it to make sure there isn't confidential information there, pc's that are partially burned who is in charge of determining if the hard drives still need to be forensically swiped instead of just letting fire department haul it all away to the dump or landfill where it could be stolen
- During renovations are contractors being supervised by bank employees and security guards or is the bank removing all customer information and data out of the bank and vaults to a different branch during the renovation process.
- How to secure the building with no alarms or a hole in a wall from fire fighters fighting the fire.
- Hire a security guard or how to secure the building and the assets (customer information) inside.

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

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.