RLI
DIFFERENT WORKS

RLI PROFESSIONAL SERVICES GROUP
PROFESSIONAL LEARNING EVENT
PSGLE 113

Emergency Preparedness & Disaster Recovery: How To Protect Your Income & Assets

Copyright Materials

This presentation is protected by US and International Copyright laws. Reproduction, distribution, display and use of the presentation without written permission of the speaker is prohibited.

© RLI Professional Services Group

RLI®

DIFFERENT WORKS

COURSE DESCRIPTION

Wherever you live and work, your firm is inevitably exposed to emergency situations. They might include natural disasters like windstorms, floods, earthquakes, or winter storms. Emergency situations can also involve man-made disasters like fires, chemical emergencies, or episodes of terrorism on varying scales. Your firm's first line of preparedness for emergency situations is to protect your own people, property, and operations.

COURSE DESCRIPTION

Your Firm's Exposure to Emergency Situations

Natural Disasters
Hurricanes
Earthquakes
Wildfires

Man-Made Disasters
Fires
Workplace Violence
Terrorism

Technology Disasters
Cyber Breaches
Software Corruption
System Failures

COURSE DESCRIPTION

Your Firm's Response to Emergency Situations

First Line of Preparedness—

Protect People, Property, Operations

Next Step—

Business Continuity

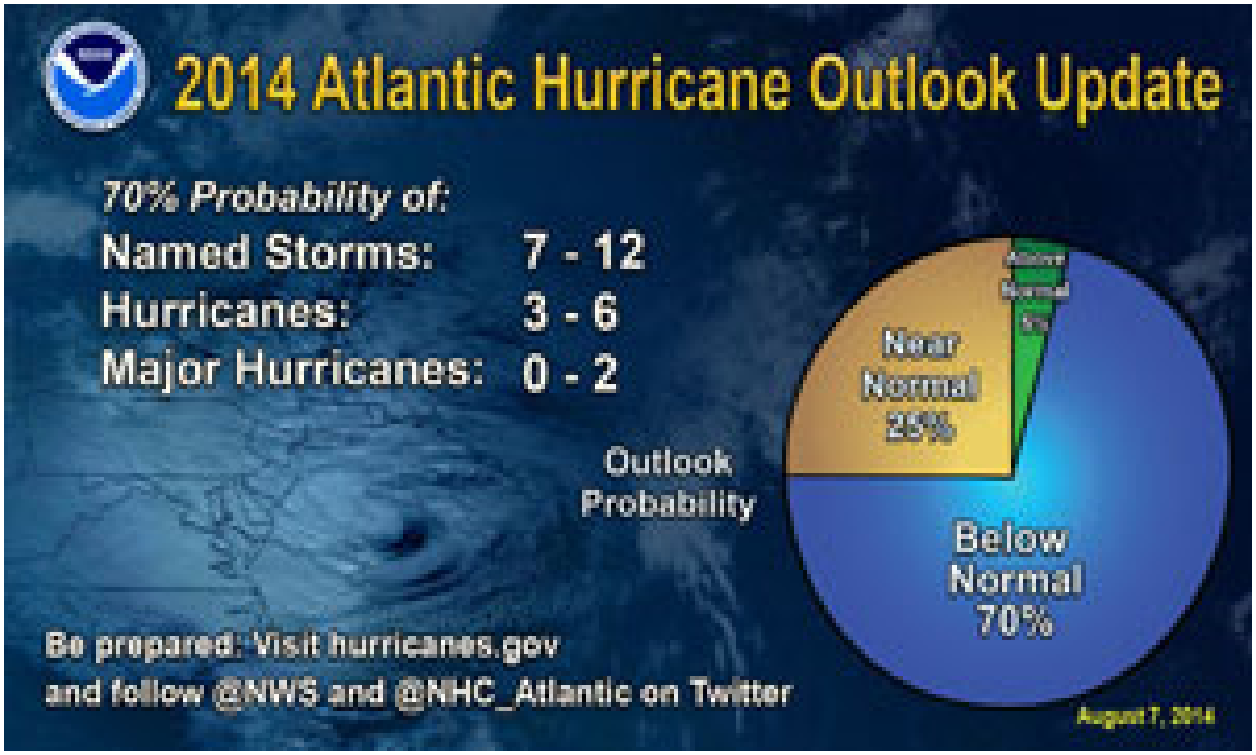
This course will outline a spectrum of emergency preparedness tips for professional services firms.

LEARNING OBJECTIVES

Participants in this course will learn more about:

- Establishing appropriate preventive measures
- Minimizing loss of life, injury, and damage to property
- Tools to manage your firm's resources
- Continuing essential functions to keep business moving

NOAA's Climate Prediction Center



NOT HAPPENING TO YOU?

2014: A Look at Disasters

- 827 Tornadoes Reported/405 Confirmed
- Hurricanes, Tropical Storms
- Polar Vortex
- Floods
  - California
  - Iowa
  - Minnesota
  - Missouri
  - New York
- Wildfires

NOT HAPPENING TO YOU?

A Look at Technological Disasters

- Computer Virus
- Software/System Failures
- Cyber Attack
- Hackers
- Theft

ANALYSIS OF COVERAGE

According to Marshall & Swift/Boeckh:

- **30%** of **Commercial Buildings** are **Undervalued by 50%**
- **50%** of **Contents** are **Undervalued by 50%**

Plus…

- In 2011, **2,941 monthly weather records were set** in the U.S. (and all states were impacted)
- **14** of those major events totaled **over $53 billion in property damages**

WHY DOES THIS HAPPEN?

Commercial Real Estate Prices Declined Beginning 2007

Typical Insurance Buyers Assume that the Cost to Rebuild or Repair has also Declined

Components of Replacement Cost have been Rising:

- Lumber Prices Rose 40% in 2012
- Other Manufacturers Followed

Catastrophes like Hurricanes and Winter Storms Cause the Cost of Supplies and Labor to Rise due to Increase in Demand

AND WHAT HAPPENS NEXT?

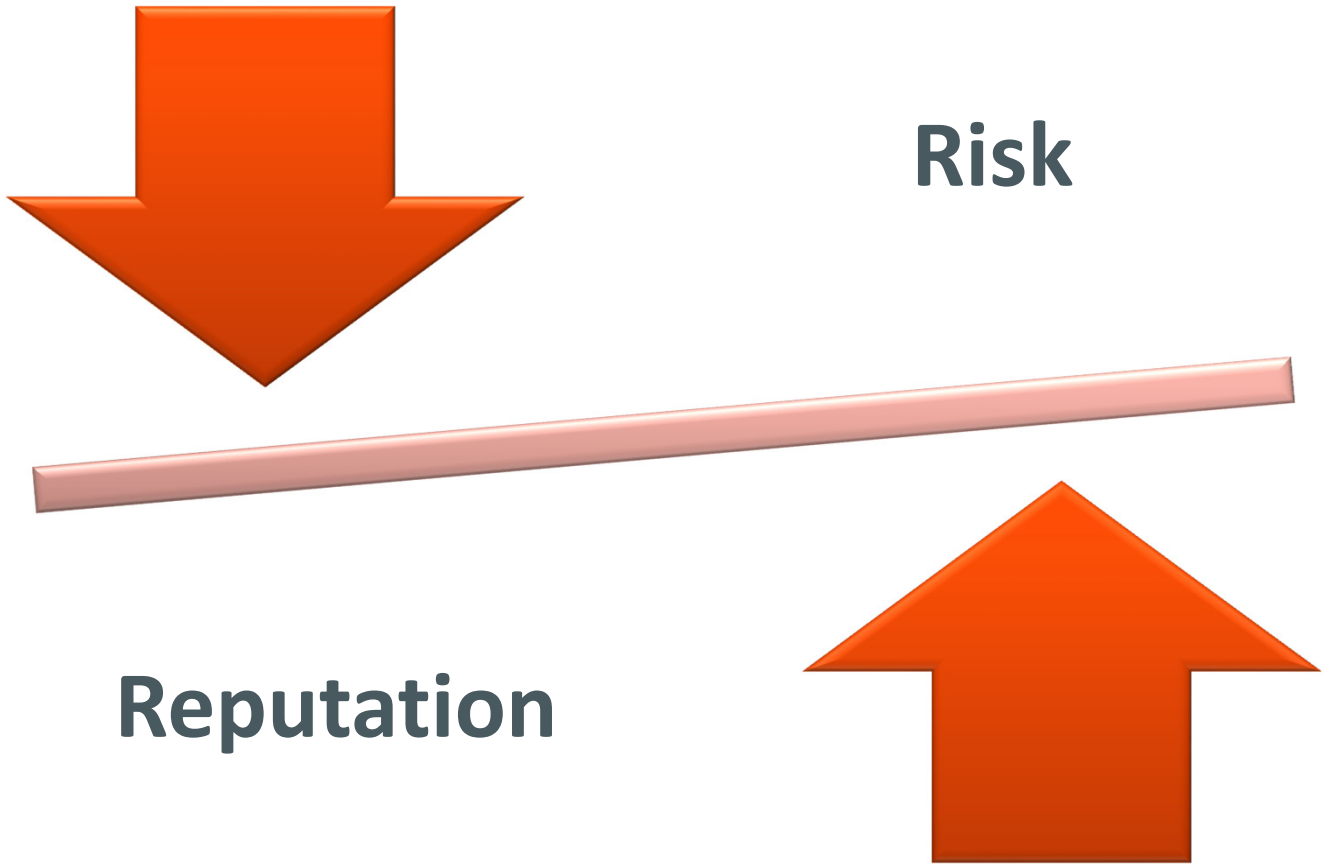
Lower Property Valuation—
and **Lower Insurance Costs**—
from 2007-2012
Helped Some Businesses Survive

- This Strategy **Only Works if a Loss Doesn't Occur**

Beyond Property Coverage,
there are **Operational Issues**
to Consider

- **75%** of companies without **business continuity plans fail** *within 3 years of a disaster*

THE RESULT?



HOW TO PLAN FOR AN EMERGENCY

Step 1: Prepare

- Establish an **Emergency Response Team**
- **Train** your Team
- Conduct **Drills** (e.g., establish a **Meeting Location**)
- Assign **Responsibilities:** **Phone Trees**—with Contingencies **Checklists**
- Maintain **Proper Response Equipment**

HOW TO PLAN FOR AN EMERGENCY

Step 2: Respond

Evacuate all Employees and Visitors:
- Evacuation Route
- Alarm System

Report Emergencies—Fire, Police, Medical:
Include Non-emergency Contacts for Local Organizations

Contact Appropriate **Regulatory Agencies**:
- Natural Disasters

Notify Appropriate **Internal Personnel**:
- Management
- Property Damage Coordinator

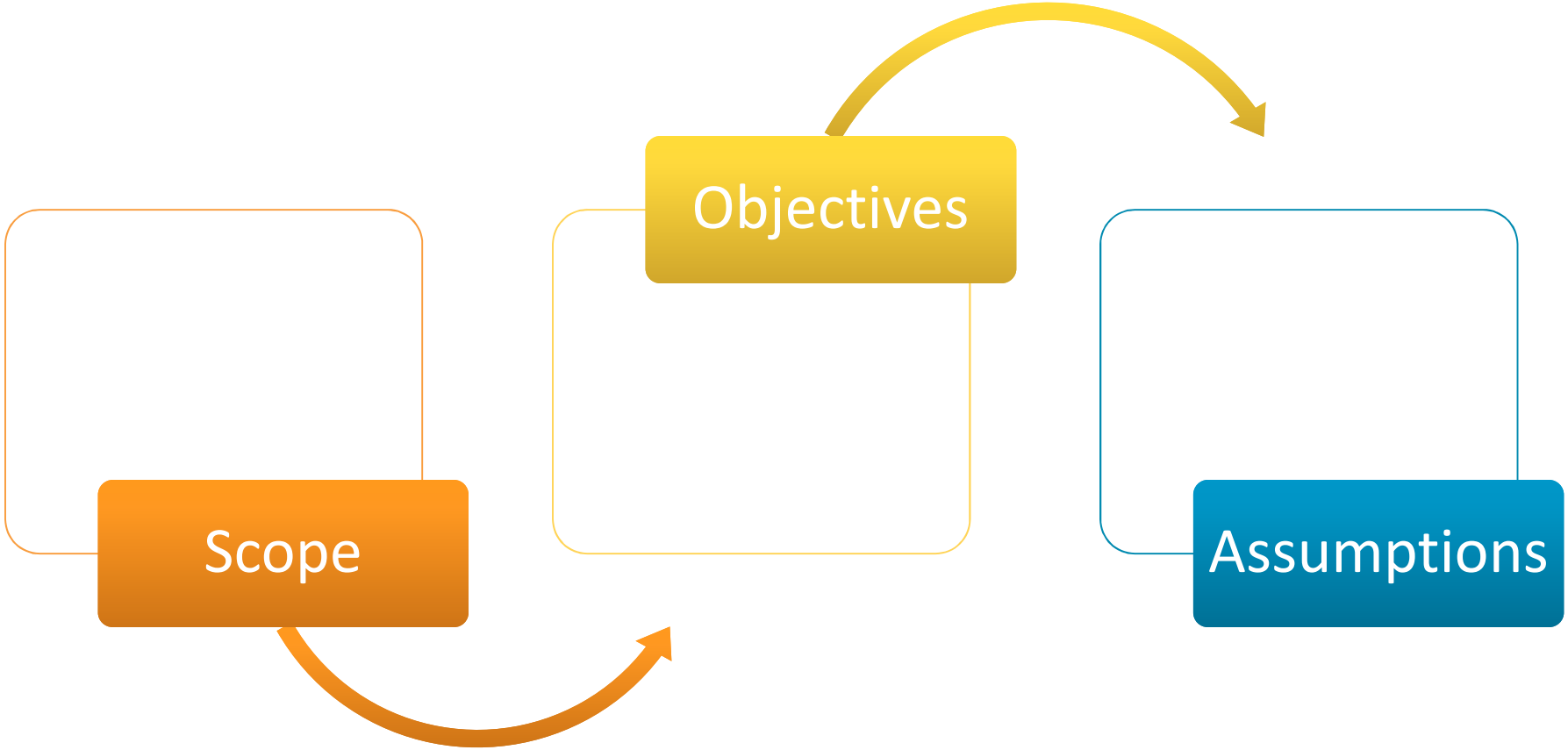
HOW TO PLAN FOR AN EMERGENCY

Steps 3 & 4: Recover and Restore

- **Search** and **Rescue**
- Salvage **Property**
- File **Reports** with Regulatory Agencies
- Employ **Business Continuity Plan**

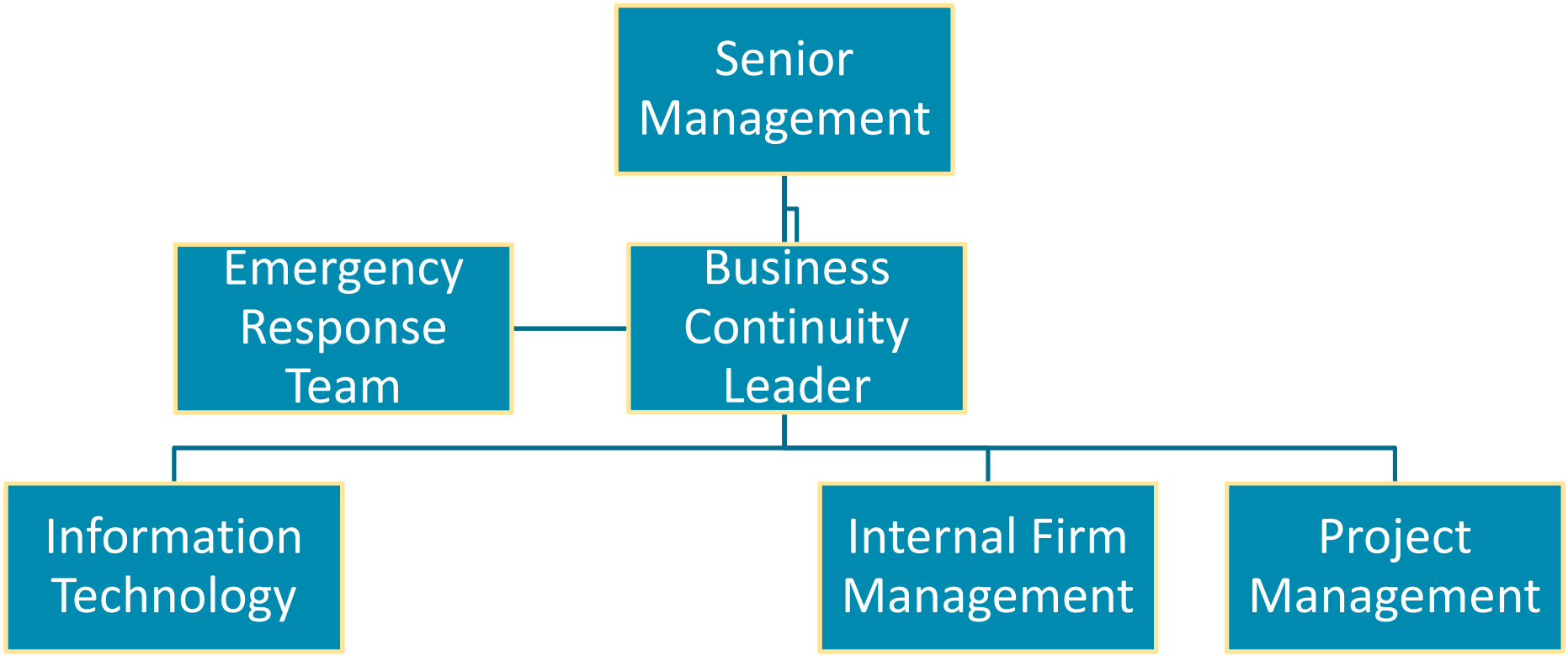
BUSINESS CONTINUITY PLANS

Step 1: Set Up the Program



Step 2: Organize the People

Roles, Responsibilities, Lines of Authority, Delegation, Coordination



BUSINESS CONTINUITY PLANS

Step 3: Analyze the Business Impact

Identify—

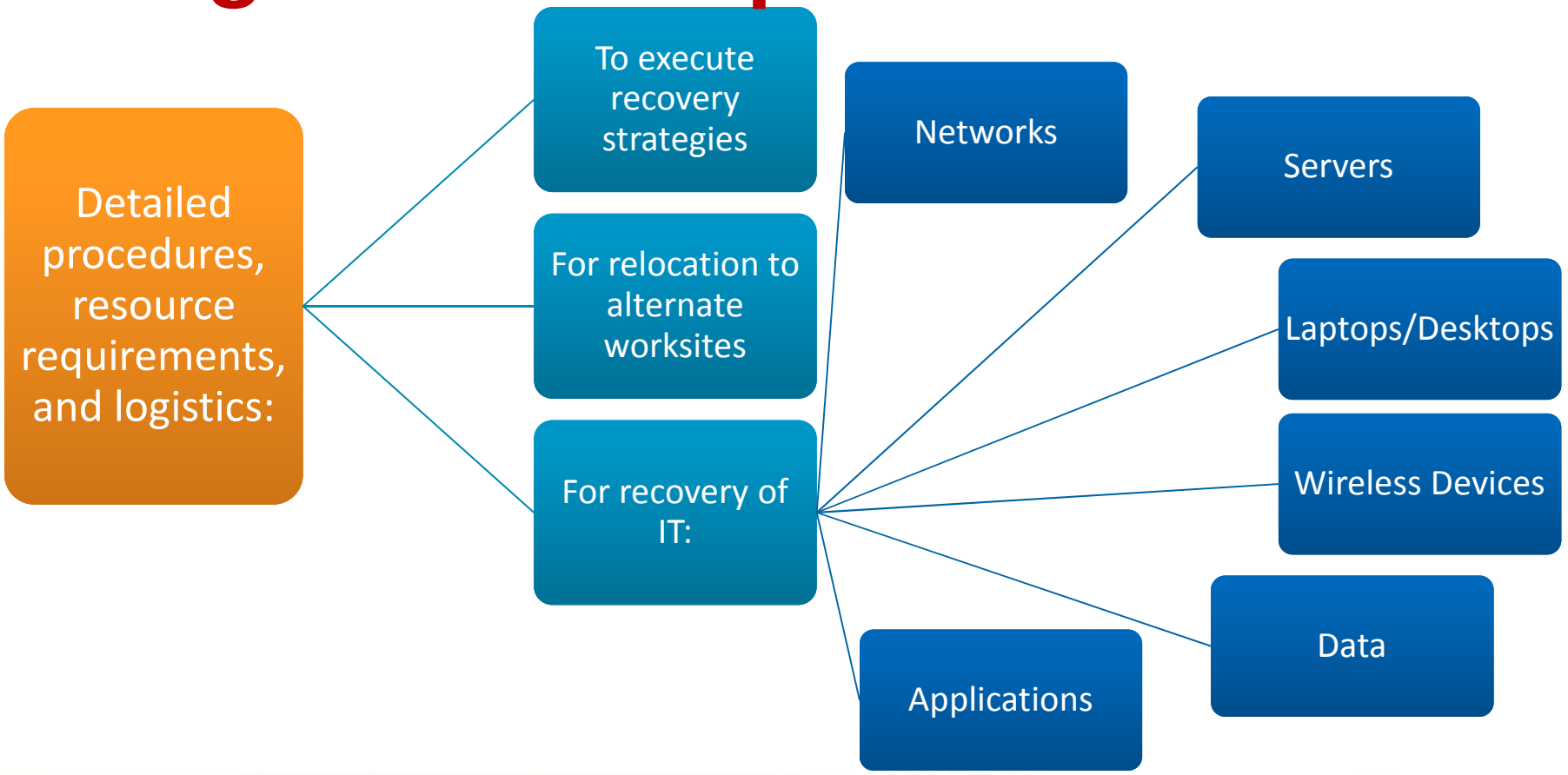
Recovery Time Objectives for:

- Business Processes
- Information Technology

Recovery Point Objectives for Data Restoration

BUSINESS CONTINUITY PLANS

Step 4: Identify Business Continuity Strategies and Requirements



BUSINESS CONTINUITY PLANS

Step 5: Create Workarounds

Document procedures for manual workarounds

Step 6: Manage Incidents

Define procedures

- Incident Detection and Reporting
- Alerting and Notifications
- Activating Business Continuity Plan
- Activating Emergency Operations Center
- Assessing Damages
- Developing and Finalizing a Plan

BUSINESS CONTINUITY PLANS

Step 7: Train & Test

Training for business continuity planners

Testing schedules, procedures, and forms

- Business recovery strategies
- IT strategies

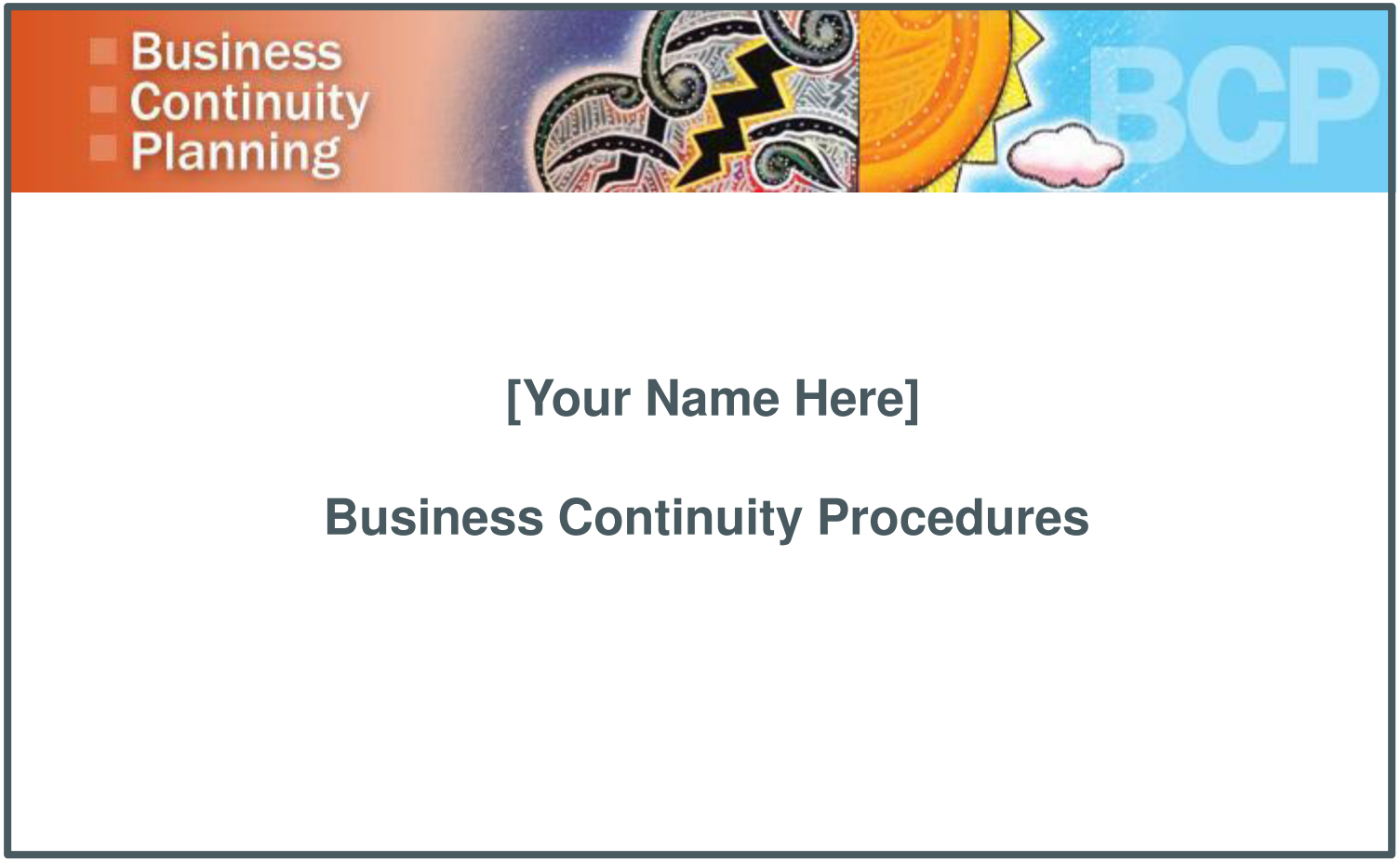
Exercises

Step 8: Maintain & Improve the Program

Schedules, triggers, and assignments for review

Corrective action to address deficiencies

Step 9: Distribute the Plan



INSURANCE COVERAGE

- Electronic Data
- Flood Insurance
- Business Income
- Extra Expense
- Contingent Business Interruption (supply chain)

CONSULT RESOURCES

www.drii.org
Disaster Recovery Institute International

www.ready.gov/make-a-plan
Federal Emergency Management Agency

Thank you for your time!

QUESTIONS??

This concludes the Professional Services Group Learning Event

RLI DIFFERENT WORKS

Laurel Tenuto, Client Risk Management Coordinator
Laurel.Tenuto@lrlicorp.com
Marie Bernier, Senior Risk Management Consultant
Marie.Bernier@rlicorp.com

THANK YOU!