CONNECTION BETWEEN RISK MANAGEMENT AND BUSINESS CONTINUITY

DECEMBER 11, 2014

Thomas Lukacs

**Director of Risk Management
New York State
Department Of Financial Services**

Manny Morales

**Information Security Officer
Office of the New York State Comptroller**

CONNECTION BETWEEN RISK MANAGEMENT AND BUSINESS CONTINUITY

Business risk

Financial Risk

Operational Risk

Business Continuity Risk

RESPONSIBILITIES

Risk Management (ERM)

- Identify mission and objectives of organizational operations
- Identify threats and vulnerabilities to the mission and objectives
- Rate risks and identify controls in place to detect or prevent risks from occurring.
- Identify gaps and develop actions to lower risk to acceptable levels.
- Communicate, train and monitor

Business Continuity

- Identifying critical functions
- Identify critical resources
- Identify potential catastrophes and vulnerabilities that threatens ongoing operations
- Develop plans to mitigate these threats and strategies for recovering if they occur
- Communicate, train and monitor

3

NYSICA

The NYS Forum, Inc.
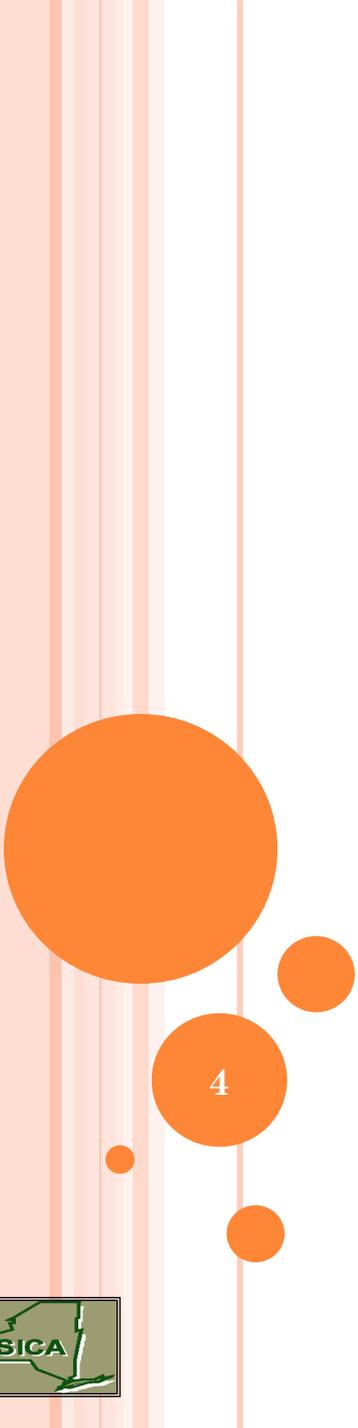
BUSINESS CONTINUITY DEPARTMENT OF FINANCIAL SERVICES

4

WHAT IS BUSINESS CONTINUITY?

- First, You Tell Us…

- Identify Critical Business Functions & Services

- Identify Critical Staff, Information & Equipment

- Document Action Plans for:

- Communication
- Protection of Staff, Information & Equipment
- Resumption of Functions & Services

5

DFS OVERVIEW

- 2011 Banking & Insurance Departments Merger

- Regulation of Banks & Insurance Industries

- 1,350~ Employees (New York City, Albany & 4 Locations)

NYSICA

The NYS Forum, Inc.

DFS Process

○ Risk Management

- Internal Control
  - IC Certification Process

- Information Security
  - Cyber Security Compliance & Reporting

- Emergency Management Planning
  - Business Continuity Planning

DFS RISK MANAGEMENT PROCESS

- New Process in 2014

- Start with Internal Control in January
  - Business Continuity Embedded

- Push Business Continuity in April
  - 30 Business Units
  - Facilitated by IT & Risk Management Directors

- Launch Cyber Security Awareness in November
  - Roll-Out Multi-Pronged Campaign

8

BCP AS AN INTERNAL CONTROL

- Like Any Good Management Practice, BCP is an Internal Control

- BCP Viewed Through an IC Lens:

  - Control Environment
  - Risk Assessment
  - Information & Communication
  - Control Activities
  - Monitoring

9

HOW TO…KEY STEPS

- Executive Support
  - Governance Process – Created EMPC
- Communications & Marketing
  - Email to Business Unit Leads
  - Unit by Unit Kick-offs and Follow Ups
  - Employee Hotline & NY-Alert
  - Evacuation Packs

NYSICA

The NYS Forum, Inc.

- Don't Reinvent the Wheel
  - Relied on IC Risk Assessment
  - Build on Prior Experience (Sandy, 9/11 etc.)

- Make Business Unit's Think It Through!
  - Questionnaire…But No Template

- Next Steps…
  - Training & Awareness
  - Exercises/Drills
  - Maintenance – BCP Certification Highlighted in Annual IC Certification

11

BUSINESS CONTINUITY OFFICE OF THE NEW YORK STATE COMPTROLLER

12

OSC PROCESS

- The process is composed of three parts
  - Emergency Management
    - Health and Safety
  - Business Continuity
    - Continuation of critical business operations
  - Disaster Recovery
    - Recovery of the Data Center and other IT infrastructures

- Then came Hurricane Sandy

OSC Objectives 2013 -2014

- Complete assessment of Hurricane Sandy's impact

- Meet with all divisions on their BC plans

- Purchase a tool for BC plans/communications to staff

- Have completed BC plans by end of summer

- Perform tests

OSC CHALLENGES

- Reviewing not just the Critical business processes

- Assigning Liaisons, loss of SMEs, Leadership changes

- Competing Business priorities

- Some businesses did not have any documented plans

- Pervious tool to create the plan, caused anxiety

- Aggressive schedule to complete

NYSICA

The NYS Forum, Inc.

ACTIONS TAKEN

o Establishment of a temporary Steering committee

o Bringing in a Consultant to assist

o Having kickoff meetings with the stakeholders

o Assigned Liaisons to work on recovery plans

o Testing of those plans (Tabletop exercise)

o Purchased a Recovery Planner tool for plans

o Improve the Disaster Recovery process

16

NYSICA

The NYS Forum, Inc.

CURRENT STATUS

- 19 major business processes with recovery plans

- Performed tabletop exercises

- Full recovery of large critical systems

- Plans are being migrated to the recovery tool

- Moving into a maintenance mode

IN SUMMARY

- Executive Buy-in

- Takes dedicated staff

- Need to look at all business processes

- Need to continue to maintain importance

- Perform a BC Health Check
  - http://www.nysforum.org/resources/bcphealthcheck/
  - www.ready.gov
  - www.fema.gov
  - http://www.nyc.gov/html/oem/html/home/home.shtml

NYSICA

The NYS Forum, Inc.