Western Intergovernmental Audit Forum

Business Continuity &
Disaster Recovery Planning

September 12, 2013

Presented by:
City of Phoenix – City Auditor Department
Aaron Cook, Sr Internal Auditor – IT Audit
Heather Kneale, Internal Auditor
Stacey Linch, Internal Auditor

How Prepared Are You?

RUN A SIMULATION OF OUR PRODUCTIVITY IF WE LOST HALF OUR WORKFORCE TO A PANDEMIC.
SHOULD I ASSUME WE LOSE THE PRODUCTIVE PEOPLE OR THE PEOPLE WHO ASK OTHER PEOPLE TO RUN PANDEMIC SIMULATIONS?
TRY BOTH WAYS.
OKAY. I'M DONE.
www.dilbert.com
scottadams@aol.com
6-15-07 © 2007 Scott Adams, Inc./Dist. by UFS, Inc.

Objectives

- Defining Business Continuity
- Defining Disaster Recovery
- Importance of BCP & DRP
- Developing a BCP and DRP
- Auditing a BCP and DRP
- Audit Resources

Key Concepts

- Emergency/Incident Plans
  - Plans developed by first responders and public safety to address disasters
- Business Continuity Plan (BCP)
  - Process to ensure business risks are identified, mitigated, and planned for so that operations can recover in response to a disruption
  - Analysis -> Strategy Design -> Implementation (Training) -> Testing -> Maintenance
- Continuity of Operations Plan (COOP)
  - Documented plan, usually using the FEMA COOP framework and templates
  - Ensures continuous availability so operations can continue
  - Ensures continuation of leadership by establishing an order of succession of key personnel
  - Specifies plans for delegation of agency authority and devolution
- Disaster Recovery Plan (DRP)
  - Plans specific to IT systems

Standards

- Disaster Recovery Institute International – DRII Professional Practices Framework
- International Organization for Standardization – ISO22301:2012
- Business Continuity Institute – Good Practices Guidelines

Business Continuity Plan

You need a plan before it's needed

Business Continuity Plan

- Goals
  - Protect Human Life
  - Protect Vital Assets
    - Property
    - Data
- Resume business operations at alternate site (if primary site inoperable)
- Restore business operations to primary site

Elements of a BCP

- BCP Committee (executive support)
- Policies and Procedures (roles and responsibilities)
- Identify Essential Functions/Services
  - Risk Assessment
  - Business Impact Analysis
  - Prioritization
- Identify Interdependencies
  - Internal/external
- Determine Succession/Delegation of Authority

Elements of a BCP cont'd

- Locate Alternate Facilities & Resources
- Determine Vital Records
- Build the Emergency Response Team (ERT)
- Conduct Staff Training
- Regular Testing, Maintenance, & Auditing
  - Tabletop Exercises, call trees, partial drills, full drills
- Communications Plan

Business Continuity Plan Importance

- Pandemic
- Power outage
- Fire
- Flood (pipes, monsoon)
- Natural gas leak
- Chemical spill (railroad, highway, chemical plant)
- Natural disaster (haboob, earthquake, tornado, hurricane)
- Nuclear explosion (power plant – Japan)
- Terrorist attack (Boston marathon)
- Wildfires/Loss of staff
- Plane crash

Yosemite fire
imperils SF's
water supply

MASSIVE MONSOON STORM
HITS VALLEY WITH DUST, RAIN

Gusts up to 62 mph reported;
thousands left without power

**Fukushima water
that is radioactive
creeps near Pacific**

**Flooding in Manila
recedes; thousands
of residents leave**

Hot Winds Wreak
Havoc in State
Power Outages

Auditing the BCP

- Audit Objectives:
  - Determine if the plan is effective and aligns to business objectives
  - Ensure the plan is consistent with accepted practices and controls
  - Ensure the plan is documented, readily available, understood by staff, and actionable
  - Validate the adequacy, completeness, and appropriateness

BCP Audit Validation

- Designated committee/emergency response team
- Policies, mission statement, recovery expectations (do business and IT align)
- Risk assessment/Business impact analysis
- Documented plan with continual updating
- Hardware and software inventory
- Designated alternate work site(s)
- Emergency procedures
  - Communication plan
  - Emergency phone numbers
- Service level agreements with external agencies
- Training, tests and drills

Disaster Recovery Planning

‘Prevention is better than a cure’

Definition and Why

- Disaster Recovery Plan Definition:
  - *Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.*

- Why?
  - Maintain data confidentiality, integrity, and availability
  - Continue providing services
  - Protect reputation and public confidence
  - PCI compliance and financial reporting
  - Protect physical assets

Key Terms

- Recovery Time Objective (RTO)
  - The time that it takes for a system to be completely up and running in the event of a disaster. The maximum time the business can afford to be without a system.
- Recovery Point Objective (RPO)
  - The ability to recover files by specifying a point in time to restore the backup copies. Describes what data (i.e., age) that will be restored in the event of a disaster.
- The RTO and RPO should align with the requirements of the business.

Standards Specific to IT

- ITIL® – Information Technology Infrastructure Library – v3 Service Design
- COBIT® 5 –DSS04 Manage Continuity
- NIST SP800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- ISO 27002:2005 – Business Continuity Management

Disaster Recovery Plan Importance

I'M PLEASED TO REPORT ANOTHER STELLAR WEEK OF ACCOMPLISHMENTS!
E-mail: SCOTTADAMS@AOL.COM
S.Adams
I MOVED MORE THAN 800,000 BITS OF DATA TO A DISASTER RECOVERY BACK-UP FACILITY!
© 1998 United Feature Syndicate, Inc.
7/11/98
DID YOU JUST TAKE CREDIT FOR COPYING A FILE TO A DISKETTE?
IT WAS MY RÉSUMÉ.

Disaster Recovery Plans Importance

- Technology failure – natural disaster, human error, virus
  - ▫ November 19, 2012 – *"Hurricane Sandy leaves wounded servers in its wake"* – (Computerworld.com)
  - ▫ August 26, 2013 – *"China's Internet hit by biggest cyberattack in its history"* – (CNNMoney)
  - ▫ August 26, 2013 – *"Server Crash Spurs Three-Hour Nasdaq Halt as Data Link Lost"* – *(BloombergBusineessweek)*

Framework

- Everyone looks to the IT department
  - Framework needed
  - Framework should include all elements to resume business process
    - Accountability, communication, escalation, recovery strategies, service levels, emergency procedures

I WAS JUST WONDERING, DO WE HAVE A DISASTER RECOVERY PLAN?
IT DEPT
© D.Fletcher for CloudTweaks.com

Disaster Recovery Plan Elements

- Disaster Recovery Team
- Staff training
- Backup Data
- Risk Analysis/Business Impact Analysis (BIA)
- Application Criticality
- Service Level Agreements
- Required hardware and software
- Third party contracts

Disaster Recovery Plan Elements

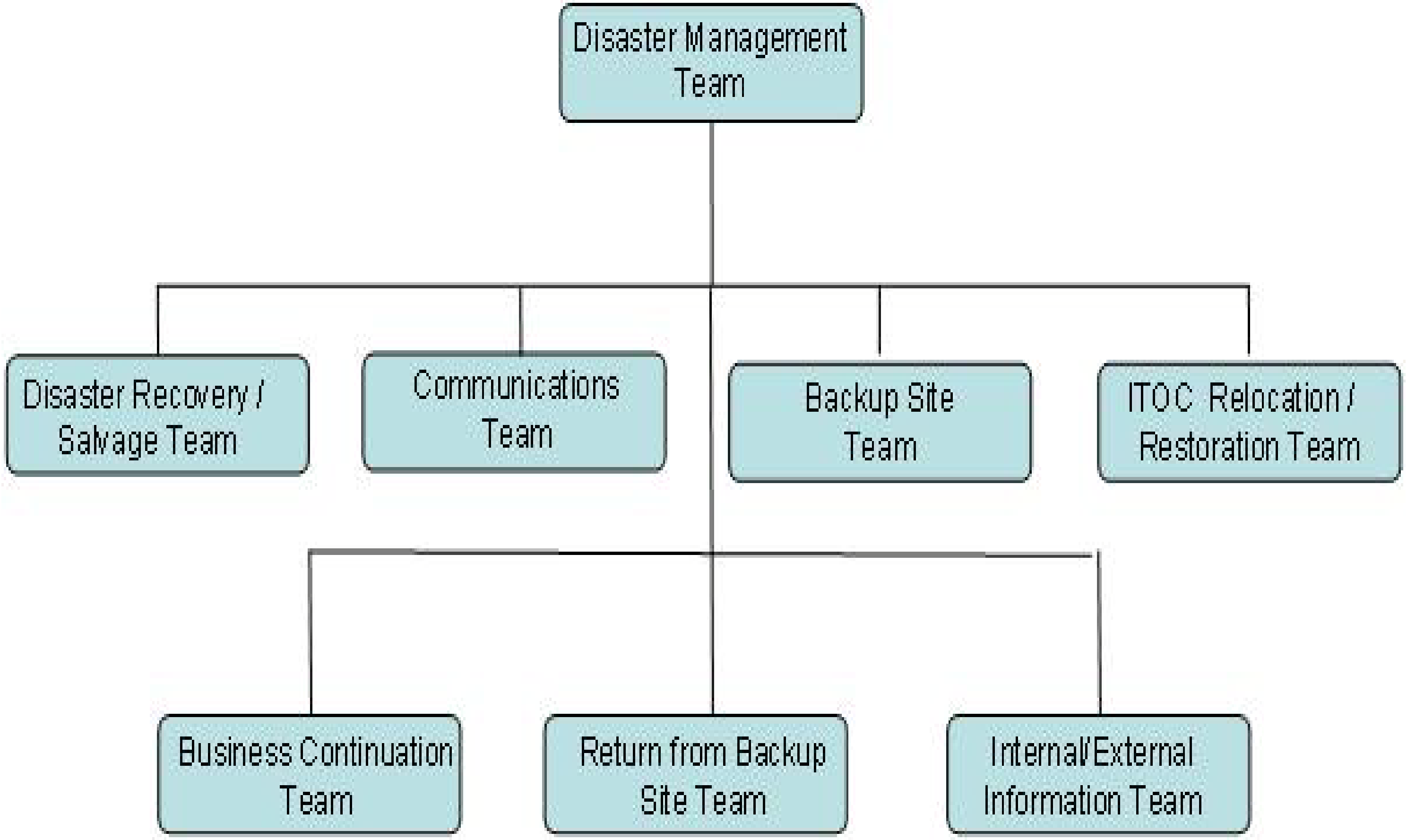
- Response/Recovery teams – roles and responsibilities
- Restoration plans
- Communication plan
- Alternate site(s)
- Plan maintenance
- Plan testing

Disaster Recovery Plan ----what should it look like?

Disaster Recovery Plan Audit Validation

- Roles and responsibilities
  - Teams
    - Incident Response, Emergency Response, Recovery , Communications, Supplies, Salvage
    - Do staff know what their roles are?
    - Is Training provided?

Disaster Recovery Plan Audit Validation


Disaster Management Team
Disaster Recovery / Salvage Team
Communications Team
Backup Site Team
ITOC Relocation / Restoration Team
Business Continuation Team
Return from Backup Site Team
Internal/External Information Team

Disaster Recovery Plan Audit Validation

- System Recovery
  - Service level agreements
  - RTO/RPO
  - System requirements
  - Restoration plans
  - Regulatory requirements
  - Back up data

Disaster Recovery Plan Audit Validation

- Data Backup
  - Availability of data
  - Offsite data
    - Security
  - Quality of data
- Plan Documentation and Accessibility
  - Online
  - Hardcopy
  - Offsite

Disaster Recovery Plan Audit Validation

- Plan Maintenance
  - Updates/Upgrades
  - New Staff
  - Change Management
  - Frequency

I THINK WE MAY NEED TO UPDATE OUR DISASTER RECOVERY PLAN. THIS ONE SUGGESTS WE ALL RUN AROUND IN CIRCLES SHOUTING 'WHAT DO WE DO?!!' 'WHAT DO WE DO?!!'

Disaster Recovery Plan Audit Validation

- Plan Testing
  - Types of testing
  - Frequency of testing
  - Documentation of testing

Lessons Learned

- Groups want to do the right thing – time, resource, and tool constraints
- Aligning business needs/expectations with IT is key
- An untested plan = No plan
- Plan maintenance – an unmaintained plan is a paper weight
- Disasters do happen

Audit Resources

- IIA’s GTAG 10 – Business Continuity Management
- ISACA’s Business Continuity Management Audit/Assurance Program
- FFEIC (Federal Financial Institutions Examination Council) IT Examination Handbook – Business Continuity Planning
- NIST SP800-53 – Contingency Planning Policy & Procedures

Questions?

- Aaron Cook – aaron.cook@phoenix.gov
- Heather Kneale – heather.kneale@phoenix.gov
- Stacey Linch – stacey.linch@phoenix.gov