DISASTER RECOVERY/BUSINESS CONTINUITY AUDITING: A CASE STUDY

WAYNE PURVES
DIRECTOR

CHRISTA VOIE
IT AUDITOR

MULTICARE HEALTH SYSTEM
TACOMA, WA


www.ahia.org
Learning Objectives

- Explain Disaster Recovery (DR) and Business Continuity Process (BCP) core concepts and critical risks.
- Share best practices in DR and BCP auditing approaches.
- Discuss the unique considerations when auditing DR and BCP requirements within the healthcare industry.
Presenters

- **Wayne Purves**, Director – Corporate Compliance and Internal Audit
  - Certifications: MBA, CIA, CISA, CFE, CHC, CRMA
  - 20+ years experience in internal audit, regulatory compliance, risk advisory and consulting

- **Christa Voie**, IT Auditor – Corporate Compliance and Internal Audit
  - Certifications: CISA, PCIP
  - 10 years experience in internal audit, compliance, finance and accounting
MultiCare Health System (MHS)

- Located in Tacoma, Washington, serving Pierce and South King County regions
- 5 Hospitals, 100+ Clinics with Diagnostic Imaging Centers and Laboratory Services
- 9K+ employees, $1.6B Annual Revenue
Presentation Outline

- Definitions
- Setting the Stage: Healthcare Industry
- Our Approach
  - Current Environment
  - Frameworks
- Scope, Objective, Audit Program
- Lessons Learned / Other Considerations
Question

What comes to mind when you think about disaster preparedness in the workplace?
What is Disaster Recovery?

- Disaster Recovery (DR) is the process of rebuilding your operation or infrastructure after the disaster has passed. (SANS Institute)
What is Business Continuity?

- Business Continuity (BC) refers to the activities required to keep your organization running during a period of displacement or interruption of normal operation. (SANS Institute)

- BC is the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. (ISO 22301:2012)
In emergencies, the community runs **TO** a hospital, **NOT** away from it!

- Caring for patients, visitors, employees, community
- Criticality for testing surge plans, simulations
- Practice, training, more practice, and more training!

**Integrated Electronic Medical Record System**

- 24x7 operations (hospitals) vs. limited hours (clinics)
- Simultaneously offline – limited paper records
- Downtime procedures = Possible lives saved!
Our Approach: Assess Current Environment

- Comments from prior IT risk assessment
- Corporate communications
- Discussions with Information Services department
- Internal Survey
Our Approach: Select A Framework

- Option: Kitchen Sink / FishNet Approach
  - “I **NEED EVERYTHING** I can find on the topic.”
  - Result: Overwhelmed. Forced to sift out essentials.

- Option: Default Approach
  - “Just use COBIT. I always use COBIT.”
  - Result: Decide v4 vs. v5, may not align with company standards or have buy-in with client.

- Option: Selective / Hybrid Approach
  - “Use a mix of select sources with the most authority.”
  - Result: Winning combination!
Our Approach: Selected Frameworks

- Joint Commission Standards
  - Emergency Management Chapter
  - Information Management Chapter
- MHS Company Policies
  - Technology: Disaster Recovery policy
  - Comprehensive Emergency Management Plan (CEMP)
- COBIT 5 Framework
  - DSS04 – Manage Continuity
Audit Scope

- Technology disaster recovery program, including planning and testing efforts for critical systems and applications.

- Centralized activities for managing business continuity plans, including the overall continuity strategy, development and testing of the emergency management plans, staff training, and communications.
Audit Objective

- To assess whether MHS has established and tested a comprehensive business continuity and technology disaster recovery strategy.
- To assess whether MHS could resume critical operations in response to a declared disaster or emergency event.
Audit Program

- Disaster Recovery
  - Technology Recovery Strategy
  - Business Impact Analysis
  - Recovery Objectives
  - Test Plans and Schedules
  - Test Results and Remediation

- Business Continuity
  - Continuity Strategy
  - Continuity Plans and Procedures
  - Communications
  - Training
DR - Technology Recovery Strategy

- Review the strategy for managing recovery of technology and systems.
- The process for managing the data centers and recovering servers during an emergency.
- Recovery processes for non-IS managed systems.
Review the Business Impact Analysis (BIA) and verify:

- It is current
- It is complete
- It documents risks and outcomes

Update the BIA after major changes.
Review the recovery objectives and timelines for system downtime and minimizing lost data.

- **Recovery Time Objective**
  - Maximum tolerable time limit within which the data must be recovered.

- **Recovery Point Objective**
  - Maximum tolerable data loss that is acceptable in a disaster situation.
DR - Test Plans and Schedules

- Review process for scheduling and planning disaster recovery tests.

- Review a sample of Mission Critical systems to verify:
  - Test plans exist
  - Test plans are current
  - Test plans identify responsibilities and actions
Review a sample of Mission Critical systems to verify:

- Recovery testing has occurred
- Testing is documented
- Post-exercise reviews were documented, with recommendations to improve continuity identified
Audit Program

- **Disaster Recovery**
  - Technology Recovery Strategy
  - Business Impact Analysis
  - Recovery Objectives
  - Test Plans and Schedules
  - Test Results and Remediation

- **Business Continuity**
  - Continuity Strategy
  - Continuity Plans and Procedures
  - Communications
  - Training
BC - Continuity Strategy

- Review the enterprise-wide business continuity strategy and processes including:
  - Corporate emergency management plans
  - Management oversight/governance
  - Hazard vulnerability assessments (HVAs)
  - Hospital planning for 96-hours of self-sustainment
  - Partnership with community resources
  - Tracking/management of emergency supplies and equipment
Emergency plans in place for each hospital/facility.
- Current
- Approved by Management
- Coverage for offsite locations, clinics
Review emergency operations plans and validate they:

- Exist
- Are current
- Define key roles, persons
- Outline procedures/actions to be performed
- Have associated test results / lessons learned
  - Includes defined follow-up, assigned actions and owners
Review that testing occurs twice annually for each hospital (per Joint Commission requirements).

Tests include:

- A simulation of a surge/influx of patients
- The local community is unable to support the hospital
- Participation in a community-wide exercise
BC – Communications

- Review the tools and processes for managing communications during an emergency.
- Review processes for maintaining current contact information.
- Review processes during an emergency response exercise to monitor and assess the effectiveness of communications (both internal and with external entities).
Notification processes in place for:

- Staff & personnel
- Patients/Families, esp. if relocating patients
- External authorities
- Media/Community
- Vendors/Suppliers
- Regional healthcare partners
BC – Training

- Review employee training on emergency practices.
- Training on emergency equipment and supplies.
- Managing emergency volunteers.
  - Licensed independent practitioners
MHS Lessons Learned

- Corporate Executive Buy-In / Executive Advocacy
  - Tell a Compelling Story – Mercy Hospital in Joplin, MS
  - Associate risks and impact of issues with organization’s mission (MHS: Quality Patient Care)
    - Actual disruptions to business continuity assisted with this point
  - Incorporate ERM Efforts to promote preparedness
  - Ask Management: “Do we want to be the hospital system that evacuates or stands firm during an emergency?”
MHS Lessons Learned (cont.)

- Business Impact Analysis
  - Process managed through I.S. or within Operations?
  - I.S. assumes priorities on behalf of Operations.
    - Disconnect between priorities, recovery timelines
    - “What are the mission critical systems?” – Different answer depending on who you ask
  - General (but undocumented) understanding of actual impact/risks to operations in the event of system downtime.
Sample Selection

Even if policy states all ‘Mission Critical’ systems require the same standard for continuity, try to include judgmental sampling to include major EMR system/s, not just select a random sample.
Other Considerations

- Understanding Hospital Incident Command System vs. Business Continuity
  - Client confusion on differences
    - HICS – Centralized Communication/Framework for Control
    - BC – Overall continuity activities, includes HICS

- Resource Plans
  - 96 hour Self-Sustainability Rule
  - Single resource provider and proximity plans
    - Back-up, and back-up to the back-up...
Resources

- Addendum 1: MHS DR/BC Audit Program
- FEMA – Federal Emergency Management Agency
  - NIMS – National Incident Management System
- State Emergency Management Department
- State Laws
  - Revised Code of Washington (RCWs)
- Local County Requirements
- OSHA – Occupational Safety and Health Admin.
Resources (cont.)

- OMB Circular A-133
- Joint Commission Standards
  - Emergency Mgmt, Info Mgmt Chapters
- COBIT 5 Framework – DSS04 (Manage Continuity)
  - www.isaca.org
- Mercy HealthCare System (Joplin, Missouri)
  - YouTube: “Mercy/ROi Joplin Story”
- The Business Continuity Institute
  - www.thebci.org
Resources (cont.)

- SANS Institute – Info Sec Reading Room
- The Institute of Internal Auditors – Global Technology Audit Guide
  - GTAG #10 – Business Continuity Management
Thank you!

Wayne Purves  
Wayne.purves@multicare.org, (253) 459-7865

Christa Voie  
Christa.Voie@multicare.org, (253) 459-8171
Save the Date
September 21-24, 2014

ahia
Assoc. of Healthcare Internal Auditors

33rd Annual Conference
Austin, Texas