

UT Southwestern Medical Center

The University of Texas Southwestern Medical Center Business Continuity/Disaster Recovery

Internal Audit Report 16:32

December 7, 2016

Table of Contents

I. Executive Summary	3
• Background/Objectives and Scope	3
• Conclusion	4
II. Detailed Observations and Action Plans Matrix	7
III. Appendices	11
• Appendix A – Risk Classifications and Definitions	11
• Appendix B – Business Continuity Program Elements	12

Executive Summary

Background

In the event of a disaster or business interruption, business continuity is the process for resuming critical operations to reduce overall impact to the business. The disaster recovery process involves the restoration of critical business applications to support the business continuity effort.

The Office of Safety and Business Continuity (OSBC) manages and oversees the UT Southwestern Business Continuity (BC) Program. In 2014, Emergency Management was restructured under the Office of Environmental Health & Safety. In October of 2015, the Offices of Environmental Health & Safety and Business Continuity were combined under the Assistant Vice President for Safety and Business Continuity creating the OSBC department. Then, the OSBC began the process of rebuilding the program from the ground up to its current state.

UTSW Policy SEC-251 Business Resilience and Texas Administrative Code (TAC), chapter 202, Information Security are the two applicable state policies mandating compliance. TAC 202 requires UT Southwestern executive management to support the Chief Information Security Officer's responsibility to guard the business operations and business assets. The SEC-251 Business Resilience policy assigns department plan owners with primary responsibility for all business continuity planning activities for their respective business units, and requires annual review and updates to the plans. Applicable hospital-related federal regulations with which UTSW must comply include emergency management rules from the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) as well as a new Emergency Preparedness regulation from the Centers for Medicaid and Medicare (CMS), which requires continuity of operations planning provisions to be in place by November 2017.

The Assistant Vice President for Safety and Business Continuity has a staff of two: one Emergency Management Coordinator and a Senior Business Continuity Planner, both of whom are formally educated in Business Continuity and Emergency Management disciplines. Information Security has one Information Resources Manager responsible for coordinating the Disaster Recovery program for Information Resources. The eBRP system is the software management tool used by all departments to document their Business Continuity / Disaster Recovery (BC/DR) plans.

The Safety and Emergency Management Officer for the University Hospitals is responsible for their emergency management and business continuity program. This program must comply with Joint Commission standards and regulations and is examined annually.

Appendix B, "Program Development," depicts the industry-recognized phases of business continuity plan development. A business impact analysis is developed to assess risk; a business continuity plan is developed to address the risk; and then the plan is exercised to assess its completeness and feasibility. Appendix C illustrates the crucial necessity for maintaining revenue during a disaster.

Objectives and Scope

This operational audit was risk-based and scheduled as a part of our Fiscal Year 2016 Audit Plan. The audit focused primarily on the management of Hospital and University Business Continuity / Disaster Recovery preparedness, Information Resources data backup and security, and Information Resources data recovery.

Executive Summary

The scope period was from April 1, 2016 to the present. Audit procedures included: interviews with the Office of Safety and Business Continuity team members and Information Security staff; walkthroughs; review of policies and procedures and other documentation; and, testing and analysis of Hospital and University department data in the eBRP software system.

The objective of the review was to assess enterprise-wide Business Continuity/Disaster Recovery (BC/DR) preparedness, planning and testing, including:

- Management of departmental resources to carry out UT Southwestern BC/DR plan
- Communication and training related to UT Southwestern BC/DR plan
- Business Impact Analysis
- Metrics for key business continuity tasks identified, e.g., acceptable outage time frames, acceptable service levels following an outage, etc.

We conducted our examination according to guidelines set forth by the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

Conclusion

Overall, the medical center has implemented business continuity and disaster recovery plans in compliance with state policies and CMS/JCAHO standards. There are opportunities to increase functional maturity in several areas: conducting quality assurance reviews, developing detailed management reports to monitor department business continuity plans, and improving recovery site space planning. Considering the infancy of the BC/DR program at UT Southwestern, increasing campus resiliency is a continual process for OSBC.

Specific strengths identified during the audit include:

- OSBC management implemented the Everbridge messaging tool for instant communication and direction to all UTSW personnel in emergency situations.
- OSBC staff have conducted numerous advisory sessions across the campus regarding best practices for continuity during power outages.
- OSBC staff conducted over 105 BC Plan training sessions across UTSW between April 1, 2016 through October 31, 2016.
- OSBC staff have conducted plan evaluations for multiple department or unit-level plans, upon invitation.

Executive Summary

The table below summarizes the observations and the respective disposition of these observations in the UT Southwestern internal audit risk definition and classification process. See Appendix A for Risk Rating Classifications and Definitions.

There were no Priority risk issues identified in the audit and there were no observations with regard to the University Hospitals business continuity program. Key improvement opportunities risk-ranked as Medium are summarized below.

Priority (0)	High (0)	Medium (3)	Low (1)	Total (4)
--------------	----------	------------	---------	-----------

- **Increase Oversight and Monitoring of Departmental Business Continuity Plans** – Procedures have not yet been implemented to proactively monitor departmental business continuity plans for completeness and feasibility.
- **Clearly Identify Assigned Locations for Staff to Assemble and Resume Operations** – At least 50 department plans did not reflect locations where staff were to gather and resume operations in the event of disaster.
- **Strengthen BC/DR Plan Testing and Training Requirements** – Opportunities exist to strengthen BC/DR Plan testing and training requirements including increasing the complexity and realism of testing and requiring additional testing documentation in the eBRP system.

Management has implemented or is in the process of implementing corrective action plans. Management responses are presented in the Detailed Observations and Action Plans Matrix section of this report.

We would like to thank all the staff of the Office of Safety and Business Continuity, Information Security and the University Hospitals Office of Accreditation and Patient Safety for their ready assistance and supportive cooperation during this review.

Sincerely,

Valla F. Wilson, Associate Vice President for Internal Audit & Chief Audit Executive

Audit Team:

Gabriel Samuel, Staff IT Auditor

Jeffrey Kromer, Internal Audit Director – IT & Specialty Audit Services

Executive Summary

cc: Bruce Brown, Ph.D., Assistant Vice President for Safety and Business Continuity
Stacey Clark, Assistant Vice President, Ambulatory Care Services
Arnim Dontes, Executive Vice President, Business Affairs
Kathryn Flores, Assistant Vice President & Chief Information Officer, University Hospitals
Suresh Gunasekaran, Associate Vice President, Health System Operations
Kirk Kirksey, Vice President and Chief Information Officer
Becky McCulley, Associate Vice President & Chief Operating Officer, University Hospitals
Bruce Meyer, M.D., Executive Vice President, Health System Affairs
Dipti Ranganathan, Associate Vice President, Academic and Administrative Information Systems
Mark Rauschuber, Assistant Vice President & Chief Information Officer, Health System
Joshua Spencer, Associate Vice President & Chief Information Security Officer
Derek Trabon, Emergency Management Coordinator
John Warner, M.D., Vice President & Chief Executive Officer of Health System Affairs
BJ White, Safety and Emergency Management Officer, University Hospitals
Craig Woodward, Manager, Information Resources

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
<p>Risk Rating: Medium ●</p> <p>1. Improve Oversight and Monitoring of Departmental Business Continuity Plans</p> <p>Procedures have not yet been implemented to proactively monitor departmental business continuity plans for completeness and accuracy.</p> <p><i>Policy SEC-251 Business Resilience</i> assigns departmental plan owners with responsibility for all business continuity planning activities for their business units. While OSBC staff have made significant advancements in BC readiness, additional oversight with quality assurance reviews will enhance overall plan completeness and feasibility. Sample testing of departmental plans revealed instances of missing or incomplete information:</p> <ul style="list-style-type: none"> • Twelve of 13 (92%) without documented periodic review • Eight of 13 (62%) without complete contact details for key department staff • Four of 13 (31%) without Recovery Time Objective (RTO) and Recovery Point Objective (RPO) criteria for their applications • Three of 13 (23%) not listing their critical applications and only minimal connectivity requirements • Two of 13 (15%) not listing their critical business processes <p>The eBRP system has limited reporting capabilities and existing reports lack sufficient detail for OSBC staff to determine whether essential data is present in each department's BC plan.</p>	<ol style="list-style-type: none"> 1. Implement quality assurance procedures to periodically monitor departmental plans for completeness and feasibility. Coordinate with departmental plan owners to provide feedback and training to correct identified plan deficiencies. 2. Coordinate with the Information Security Manager and the eBRP vendor to determine feasibility and cost/benefit of additional system and reporting features to enhance quality assurance monitoring. Reports capturing key departmental plan data, such as staff training occurrence, key staff identification, BC plan completion, periodic plan review dates, and critical applications identification, etc. would be beneficial for effective OSBC management review and follow-up. 	<p><u>Management Action Plans:</u></p> <ol style="list-style-type: none"> 1. The focus of the program has been on completing the initial cycle of obtaining documented plans and ensuring the plans are tested. The process of reviewing departmental plans for potential improvements is the next step in the program's process. The program only has 1.5 FTE dedicated to Business Continuity so a sample of the plans will be reviewed on an annual basis. 2. The Business Continuity Program leaders will coordinate with Information Security, Enterprise Data Services and the eBRP software vendor to assess and evaluate software features and additional cost effective reporting capabilities so we do not have to track these items outside of the software as planned. If feasible, reports will be generated within 60 days. <p><u>Action Plan Owners:</u></p> <p>Assistant Vice President for Safety and Business Continuity</p> <p>Associate Vice President for Academic and Administrative Information Systems</p> <p><u>Target Completion Dates:</u></p> <ol style="list-style-type: none"> 1a. Procedure defined by February 28, 2017 1b. Initial sample of plans selected and plan reviews performed by May 31, 2017 2a. Evaluation completed by January 31, 2017 2b. Implementation completed by March 31, 2017

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
<p>Risk Rating: Medium ●</p> <p>2. Clearly Identify Assigned Locations for Staff to Assemble and Resume Operations</p> <p>At least 50 department plans did not reflect locations where staff would gather and resume operations in the event of disaster. Without designated recovery locations, recovery space planning may not be adequate and resumption of operations may not be possible.</p>	<p>While it cannot be predicted what area(s), on or off main campus, would be impacted in the event of a disaster, planning steps to utilize possible work space should be taken. The overall planning process should be included in the overarching institutional Continuity of Operations Plan (COOP).</p> <p>Coordinate with department Plan Owners to revise their BC plans to include alternate workspace locations to resume operations where practical and refer to the COOP as necessary.</p>	<p><u>Management Action Plans:</u></p> <p>Currently, the UTSW Emergency Management Plan explains how the “all-hazards” approach to emergency response lends itself to a faster, more efficient recovery process. This approach brings key stakeholders together when warranted to make critical, time-sensitive decisions which consider available assets and resources that are unaffected. The institutional COOP will be updated to include a process for departments to formally request alternate workspace and a group of responsible leaders to address the requests. In addition, departments with multiple locations will be instructed to include utilization of their existing alternate space in their plans as practical.</p> <p><u>Action Plan Owners:</u></p> <p>Assistant Vice President for Safety and Business Continuity</p> <p><u>Target Completion Dates:</u></p> <p>February 15, 2017</p>

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
<p>Risk Rating: Medium ●</p> <p>3. Strengthen BC/DR Plan Testing and Training Requirements</p> <p>The following are opportunities to enhance BC/DR testing and training:</p> <ul style="list-style-type: none"> • Current testing requirements for departmental plans are for table-top exercises, which are convenient, but may not be adequate to identify all weaknesses in a plan. • Training of departmental staff in their BC/DR plans is not required to be documented in the eBRP system • Currently, there is no designated section in the eBRP system to log testing of BC plans and to document lessons learned with the existing After Action Report (AAR). Without documentation, sufficient training may not be occurring and OSBC management may not be able to verify BC plan modification following each training evaluation. Further, there is confusion between the Exercise Evaluation Guide (EEG) and the AAR where some departments included the EEG instead of the AAR. 	<ol style="list-style-type: none"> 1. Enhance plan testing to require increasingly complex and realistic testing such as missing key personnel and eventually, full offsite exercises. 2. Reinforce the policy and educate all 130 departments about the importance of and diligence required for effective BC/DR plan testing. Enhance monitoring of departmental BC/DR plan training with periodic reporting to UT Southwestern executive management. 3. Explore whether it is feasible to modify the eBRP system to include a category for each department to record its staff training including the AAR document and clarify whether the EEG form should be included. Exercise the option if available. 4. Explore using the eBRP Toolkit feature for managing exercises and assigning resources. 	<p><u>Management Action Plans:</u></p> <ol style="list-style-type: none"> 1. Business Continuity practices do not specify the type of exercise to utilize, i.e. a functional exercise over a table-top drill. We believe each department should consider the merits and risks of each type of exercise and decide on the method that best meets their needs. The business continuity program will develop points to consider for departments when deciding on an exercise format. 2. The Business Continuity Program process will inform departments that documentation of training of personnel with BC responsibilities is to be uploaded into eBRP system. 3. The Business Continuity Program will inform departments that documentation of plan testing and corrective action reports is to be uploaded into the eBRP system. 4. The Business Continuity Program will coordinate with the IR Manager to evaluate features of the eBRP system which may enhance overall management of exercises, plan testing and training management. <p><u>Action Plan Owners:</u></p> <p>Assistant Vice President for Safety and Business Continuity</p>

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
		<p><u>Target Completion Dates:</u></p> <ol style="list-style-type: none"> 1. February 15, 2017 2. February 15, 2017 3. February 15, 2017 4. January 15, 2017
<p>Risk Rating: Low ●</p> <p>4. Configure Automated Plan Review Reminders in the eBRP System</p> <p>The eBRP system is not configured to send an automatic reminder to departmental Plan Owners when a periodic plan review is due. As a result, plans may have obsolete or erroneous data such as staff contact information. It is essential that all department BC plans are periodically revised and updated as a result of changes in compliance regulations, staffing, and technology.</p>	<p>Configure the eBRP system feature to send an automated reminder to department BC Plan Owners when their department plans must be reviewed and reapproved.</p>	<p><u>Management Action Plans:</u></p> <p>The Business Continuity Program will coordinate with Information Security and the software vendor to provide reminders to plan responders and owners regarding the annual plan review requirement.</p> <p><u>Action Plan Owners:</u></p> <p>Assistant Vice President for Safety and Business Continuity Manager Information Resources</p> <p><u>Target Completion Dates:</u></p> <p>February 15, 2017</p>

Appendix A – Risk Classifications and Definitions

As you review each observation within the Detailed Observations and Action Plans Matrix of this report, please note that we have included a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our review. The following chart is intended to provide information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

<p>Risk Definition - The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.</p>	<p>Degree of Risk and Priority of Action</p>	
	<p>Priority</p>	<p>An issue identified by internal audit that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.</p>
	<p>High</p>	<p>A finding identified by internal audit that is considered to have a high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.</p>
	<p>Medium</p>	<p>A finding identified by internal audit that is considered to have a medium probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level. As such, action is needed by management in order to address the noted concern and reduce risk to a more desirable level.</p>
	<p>Low</p>	<p>A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level. As such, action should be taken by management to address the noted concern and reduce risks to the organization.</p>

It is important to note that considerable professional judgment is required in determining the overall ratings presented on the preceding pages of this report. Accordingly, others could evaluate the results differently and draw different conclusions.

It is also important to note that this report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.

Appendix B – Business Continuity Program Development Cycle

The graphic below depicts the industry-recognized phases of business continuity management.

- A business impact analysis is developed to assess risk;
- A business continuity plan is developed to address the risk;
- The plan is exercised to assess the plan's completeness and feasibility;
- Modifications to the plan are then made based on lessons learned from the exercise and the cycle repeats.

