January 12, 2016

Dr. Hobson Wildenthal, President *ad interim*
Ms. Lisa Choate, Chair of the Institutional Audit Committee:

We have completed an audit of Business Continuity Planning as part of our fiscal year 2015 Audit Plan, and the report is attached for your review. The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing.* The objective of our audit was to evaluate the completeness and appropriateness of the business continuity planning (BCP) process for departments as administered by Business Services.   BCP's for departments are intended to maintain essential operations in the event of a disaster at the institution.

Based on the audit work performed, we conclude that controls over the business continuity planning process for departments are working as intended by management.   Implementation of the recommendations will help minimize the risks of departmental operations not continuing in the event of an emergency or disaster.

Management has reviewed the recommendations and has provided responses and anticipated implementation dates. Though management is responsible for implementing the course of action outlined in the response, we will follow up on the status of implementation subsequent to the anticipated implementation dates.   We appreciate the courtesies and considerations extended to us during our engagement. Please let me know if you have any questions or comments regarding this audit.

Toni Stephens
Institutional Chief Audit Executive

UT Dallas Responsible Parties:
  Dr. James Wright, Assistant Vice President of Environmental Health and Safety
  Teresa Johnston, Director of Business Services

Members of the UT Dallas Institutional Audit Committee:
  External Members:
   Mr. Bill Keffler
   Mr. Ed Montgomery
   Ms. Julie Knecht
  Dr. Inga Musselman, Acting Provost
  Dr. Calvin Jamison, Vice President for Administration
  Mr. Terry Pankratz, Vice President for Budget and Finance
  Mr. David Crain, Vice President and Chief Information Officer
  Dr. Bruce Gnade, Vice President for Research
  Dr. George Fair, Vice President for Diversity and Community Engagement; Compliance Officer
  Dr. Gene Fitch, Vice President for Student Affairs
  Mr. Timothy Shaw, University Attorney

The University of Texas System:
  System Audit Office

State of Texas Agencies:
  Legislative Budget Board
  Governor's Office
  State Auditor's Office
  Sunset Advisory Commission

Executive Summary

Business Continuity Planning, Report No. R1613

Audit Objective and Scope: The objective of our audit was to evaluate the completeness and appropriateness of the business continuity planning (BCP) process for departments as administered by Business Services. BCP's for departments are intended to maintain essential operations in the event of a disaster at the institution.		
The following is a summary of the audit recommendations by risk level. See Appendix for additional details.		
Recommendation	**Risk Level**	**Estimated Implementation Date**
(1)Ensure Business Continuity Plans Are Tested	**Medium**	March 1, 2016
(2)Separate the Duties over Creating and Approving the Plans	**Low**	March 1, 2016
Responsible Vice President: Dr. Calvin Jamison, VP for Administration	**Responsible Parties:** • Dr. James Wright, Assistant VP of Environmental Health and Safety • Teresa Johnston, Director Business Services	
Staff Assigned to Audit: Project Leader: Colby Taylor, IT Staff Auditor		

Table of Contents

Background

Business continuity plans should be in place to ensure continued operations of all critical functions in the event of a natural disaster or other emergency event. The Business Services department, reporting under the Vice President for Administration to the Assistant Vice President of Environmental Health and Safety, is responsible for assisting UT Dallas departments in developing and reviewing business continuity plans. Disaster recovery and business continuity for administrative applications, such as PeopleSoft, is handled by Information Resources.[1]

Although recent changes in TAC 202 have altered the wording on required BCP programs, there are now more specific standards available dealing with contingency planning. These new standards are issued by the Texas Department of Information Resources and can be found here: Security Control Standards Catalog. Starting on page 75 of the current document, there is a section labeled CP-Contingency Planning that lists several standards that were created to help state agencies and higher education institutions implement the various controls.

Natural disruptions and manmade outages are unpredictable, but their impact on a business may be managed if the business has invested time into starting and maintaining a business continuity planning (BCP) program. The goal of a good BCP program is to facilitate restoration of critical business process after a disaster has been declared. To achieve this goal, an organization must perform an assessment of the risks to the various business processes to establish which of the processes are critical and which are not. Once the risk assessment is completed, management will then be able to focus on the most critical areas when formulating the BCP program.
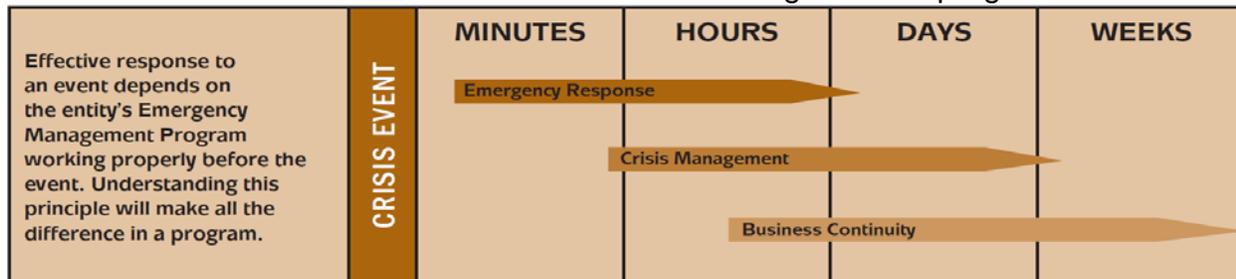

Figure 1: Typical timeline of an Emergency Management Program after a crisis event

At UT Dallas, the Kuali Ready application, administered by Business Services, is used to assist with the following BCP functions:
- Formulate BCP programs
- Store BCP programs
- Modify or change plans

Currently, the application houses about 85 business continuity plans for UT Dallas departments.

---

[1] Disaster recovery for administrative systems was not within the scope of this audit.

Audit Objective

The objective of our audit was to evaluate the completeness and appropriateness of the business continuity planning (BCP) process for departments as administered by Business Services.   BCP's for departments are intended to maintain essential operations in the event of a disaster at the institution.

Scope and Methodology

The scope of this audit was departmental BCP programs marked as completed during FY 2015, and our fieldwork concluded on November 17, 2015.   To satisfy our objectives, we performed the following:

- Gained an understanding of the departmental business continuity planning process at UT Dallas, including interviewing responsible staff
- Attended planning sessions for an in-process BCP process
- Used and investigated the Kuali tool
- Reviewed existing BCP plans from a variety of different departments/units
- Reviewed the guided process for recommended scenarios

Where applicable, we conducted our examination in accordance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance or audit work, and management of the internal auditing department.

Audit Results and Management's Responses

Controls
Our audit work indicated that the following controls currently exist:

- The BCP process is guided via the Kuali webpage.
    - Access is integrated with the UTD netid login.
- Business Services has developed training on business continuity for the University.[2]
- Completed BCP's are reviewed annually by the Business Services team.
- Approvals are required by the department head or their designated representative.
    - Upon final approval of each plan, the completed plans are emailed by Business Services to appropriate VP of the area.
- Roles with different levels of access privileges are being utilized.

---

[2] http://www.utdallas.edu/safety/download/Continuity_Planning.pdf

- o Access within the BCP tool is further restricted by internal groups which prevents everyone from editing or viewing every plan.

Audit Recommendations

Priority Findings – UT System: A UT System priority finding is defined by the UT System Audit Office as: "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"[3] We have **no UT System Priority Findings** resulting from this audit.

Although the above controls are in place, opportunities exist to enhance the completeness of the business continuity plans as outlined below.

(1) *Ensure Business Continuity Plans Are Tested*
Risk Rating: **Medium**⭐

The Business Services department currently recommends at least one exercise a year to test the business continuity plans prepared by each area. While some departments, such as Web Services, have conducted testing, the majority of individual departments and academic units are not performing any test exercises or scenarios for testing their business continuity plans. Lack of testing could result in plans not working as intended should an actual disaster or emergency event occur. Using a tabletop exercise or live scenario will help validate the business continuity plans that have been formulated.

Recommendation: Business Services should develop ways to involve management in encouraging and testing business continuity plans and consider coordinating more exercises or scenarios for departments.

Management's Response: We are currently evaluating software that will assist us in the testing of the plans. Until the software is purchased and implemented, questions will be asked at each annual review to test the plan. Cards with applicable questions have already been developed to use with each annual review.

Estimated Date of Implementation: March 1, 2016

Person Responsible for Implementation: Teresa Johnston, Director Business Services

---

[3] The appendix defines the risk levels for all internal audit recommendations.

(2) *Separate the Duties over Creating and Approving the Plans*
    Risk Rating: **Low**⭐

The current business continuity planning tool allows for the same person to create and approve the plan, and the sign-offs cannot be modified once made. The UTD Information Security and Acceptable Use policy (http://policy.utdallas.edu/utdbp3096) states: "UTD Information Systems access should be designed to maintain separation of duties to reduce the risk of a malicious individual performing conflicting activities."

Without a proper separation of duties, risks are increased that the plan may either not be complete or will fail in the event of an emergency. Business Services does review all plans; however, they are not always as familiar with the business unit's operations as departmental faculty/staff involved are.

Recommendation: Duties should be separated to ensure that one person in the department does not completing all BCP functions. Until the current version of BCP application is updated with a new version, Business Services should find ways to document the separation of duties.

Management's Response: We will be migrating to a new version of the Kuali Ready software in January/February 2016. During the training on the new software, we will discuss how to implement separation of duties. We will also make this discussion part of our annual review process.

Estimated Date of Implementation: March 1, 2016

Person Responsible for Implementation: Teresa Johnston, Director Business Services

Conclusion

Based on the audit work performed, we conclude that controls over the business continuity planning process within Business Services are working as intended by management. Implementation of the above recommendations will help minimize the risks of operations not continuing in the event of an emergency or disaster.

We appreciate the courtesy and cooperation received from the management and staff in Business Services as part of this audit.

Appendix: Definition of Risks

Risk Level	Definition
High	High probability of occurrence that would significantly impact UT System and/or UT Dallas. Reported to UT System Audit, Compliance, and Management Review Committee (ACMRC). Priority findings reported to the ACMRC are defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*"
High/Medium	Risks are considered to be substantially undesirable and pose a moderate to significant level of exposure to UT Dallas operations. Without appropriate controls, the risk will happen on a consistent basis.
Medium	The risks are considered to be undesirable and could moderately expose UT Dallas. Without appropriate controls, the risk will occur some of the time.
Low	Low probability of various risk factors occurring. Even with no controls, the exposure to UT Dallas will be minimal.