February 28, 2017

Dr. Horace Mitchell, President
California State University, Bakersfield
9001 Stockdale Highway
Bakersfield, CA 93311-1022

Dear Dr. Mitchell:

**Subject: Audit Report 16-51, IT Disaster Recovery, California State University, Bakersfield**

We have completed an audit of *IT Disaster Recovery* as part of our 2016 Audit Plan, and the final report is attached for your reference. The audit was conducted in accordance with the Institute of Internal Auditors’ *International Standards for the Professional Practice of Internal Auditing*.

I have reviewed the management response and have concluded that it appropriately addresses our recommendations. The management response has been incorporated into the final audit report, which has been posted to the Office of Audit and Advisory Services’ website. We will follow-up on the implementation of corrective actions outlined in the response and determine whether additional action is required.

Any observations not included in this report were discussed with your staff at the informal exit conference and may be subject to follow-up.

I wish to express my appreciation for the cooperation extended by the campus personnel over the course of this review.

Sincerely,

Larry Mandel
Vice Chancellor and Chief Audit Officer

c: Timothy P. White, Chancellor
IT DISASTER RECOVERY

California State University,
Bakersfield

Audit Report 16-51
December 8, 2016
EXECUTIVE SUMMARY

OBJECTIVE

The objectives of this audit were to determine whether an appropriate governance structure exists to address program and facility readiness and resource planning for the recovery of data processing services following a catastrophic event; to ascertain the effectiveness of operating controls related to information technology disaster recovery (ITDR) planning and preparedness; and to evaluate adherence to the Integrated California State University Administrative Manual (ICSUAM) business continuity and disaster recovery policy and compliance with relevant regulations, Trustee policy, and other Office of the Chancellor directives.

CONCLUSION

Based upon the results of the work performed within the scope of the audit, a few specific control weaknesses were noted; generally, however, controls were adequate, appropriate, and effective to provide reasonable assurance that risks were being managed and objectives were met.

ITDR planning is a critical function of the information technology (IT) department and a key element of the campus business continuity plan. The ITDR plan at California State University, Bakersfield was out-of-date and requires additional details as listed in the observations. Recovery planning for a campuswide disaster had not been completed; however, the campus had implemented redundant systems and facilities to mitigate local disasters affecting the primary data center.

Specific observations, recommendations, and management responses are detailed in the remainder of the report.
OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. ITDR PLAN UPDATES

OBSERVATION

The campus ITDR plan was not current and had not been updated since 2014, and the campus did not have a process to ensure that the plan was periodically updated, reviewed, and approved.

Additionally, we found that the ITDR plan did not include:

- A listing of critical business systems that would need to be restored in a disaster.
- An estimated timeline for the restoration of core infrastructure, systems, and applications, or the amount of time required to set up and install new hardware and restore data from backup media.

RECOMMENDATION

We recommend that the campus update the ITDR plan to include all key elements listed above.

MANAGEMENT RESPONSE

We concur. We will modify our ITDR plan to include timelines for restoration of core infrastructure, systems, and applications and will have an updated ITDR plan by May 19, 2017.

2. ALTERNATE PROCESSING FACILITY

OBSERVATION

The campus had not identified an off-campus alternative processing facility or another campus that would be able to house and support relocated equipment in the event that campus data centers were adversely impacted by a disaster.

RECOMMENDATION

We recommend that the campus identify an alternate processing facility or another campus that would be able to house and support relocated campus equipment in the event campus data centers were impacted by a disaster.

MANAGEMENT RESPONSE

We concur. We will identify an alternate processing facility that will be able to house and support relocated campus equipment in the event that both of our on-campus data centers are impacted by a disaster by June 30, 2017.
3. OFFSITE STORAGE

OBSERVATION

The campus did not send backup copies of data to an offsite storage location.

We found that the system backup process replicated data from one campus location to another; however, data was not sent offsite for storage.

Data restoration and recovery could be adversely affected in a campuswide disaster affecting multiple buildings.

RECOMMENDATION

We recommend that the campus send backup copies of data to an offsite storage location.

MANAGEMENT RESPONSE

We concur. We will either replicate our active data to our alternate processing facility or send backup copies of our data to an offsite location by June 30, 2017.

4. EQUIPMENT REPLACEMENT CONTRACT

OBSERVATION

The campus was not using the systemwide vendor contract for emergency equipment replacement, had not implemented a process to update and maintain the list of critical IT equipment that would need to be replaced in a disaster, and had not designated an equipment drop-off location.

In addition, we found that the campus equipment replacement contract was out of date, did not include a current list of authorized IT staff members, and had not been reviewed since 2010.

RECOMMENDATION

We recommend that the campus use the systemwide vendor contract for emergency equipment replacement, implement a process to update and maintain the listing of critical IT equipment that would need to be replaced in a disaster, and designate an equipment drop-off location.

MANAGEMENT RESPONSE

We concur. We will select a vendor that can provide emergency equipment replacement and develop a workflow process to keep the list of critical IT equipment maintained by June 9, 2017.
5. ITDR PLAN TESTING

OBSERVATION

The campus had not performed comprehensive testing of the ITDR plan.

We found that the campus had tested parts of the redundant data center capabilities; however, it had not performed thorough testing to ensure that the plan would meet recovery objectives.

Executive Order (EO) 1014 requires that the campus create a detailed recovery test plan, and that all key components of the plan be tested within a seven-year timeframe.

RECOMMENDATION

We recommend that the campus create a comprehensive ITDR test plan and a schedule for performing tests of specific components of the plan to help ensure the disaster recovery plan would meet recovery objectives.

MANAGEMENT RESPONSE

We concur. We will create a comprehensive ITDR test plan and a schedule for testing the plan by June 30, 2017.

6. BUSINESS IMPACT ASSESSMENTS

OBSERVATION

The campus business impact assessments (BIA) did not include consideration of the loss of data processing services, nor did they document departmental dependence on critical applications, systems, or hardware.

RECOMMENDATION

We recommend that the campus update its BIAs to include the impact of a loss of data processing services by specifying the number of days the campus could continue without data processing before the manual processing of services would be severely impacted.

MANAGEMENT RESPONSE

We concur. We will support our key business unit leaders to update their BIAs within Kuali Ready by June 30, 2017.
7. MANUAL PROCESSING DOCUMENTATION

OBSERVATION

Campus business departments had not documented manual desk procedures required to conduct business in the event that data-processing services were disrupted, nor did they have instructions about how to re-create lost data.

RECOMMENDATION

We recommend that the campus business departments document manual desk procedures required to conduct business in the event data-processing services are disrupted, as well as instructions on how to re-create lost data.

MANAGEMENT RESPONSE

We concur. We will support our key business leaders to document manual desk procedures needed to support operations in case of a data-processing disruption and will document their processes for re-creating data by June 30, 2017.

8. IT STAFF EMERGENCY TRAINING

OBSERVATION

The campus did not train data center staff to properly operate data center emergency equipment.

Employees who periodically work inside the data center should be trained to operate the data center emergency equipment to ensure employee safety and reinforce emergency protocol.

RECOMMENDATION

We recommend that the campus train data center staff to properly operate data center equipment during an emergency or disaster and reinforce employee safety and emergency protocol responsibilities in the event of a disaster.

MANAGEMENT RESPONSE

We concur. We will train data center staff on proper use of emergency equipment and processes annually and will perform the first training and finalize documentation by May 19, 2017.
GENERAL INFORMATION

BACKGROUND

ITDR planning is a specific subset of the campus business continuity planning process that addresses how the IT resources required to operate critical business functions will be restored in a timely and effective manner following a disaster. ITDR planning requires the interaction of individuals at every level of an organization and a recognition by the organization that, in today’s computer-driven work environment, the loss of data-processing capabilities can lead to significant financial loss and non-financial exposures if an organization has not planned properly for such an occurrence.

The ITDR planning process requires the evaluation and consideration of several factors, including:

- Who will coordinate the recovery activities, and which supporting groups will report to that coordinator.
- How business units will be impacted if data-processing capabilities are lost.
- Which IT systems are critical to support those business units.
- How systems will be restored in the event of a disaster, whether alternate processing facilities will be necessary, whether backup hardware should be stockpiled, and whether insurance coverage will be needed to cover the costs of recovery activities.
- The kind of training individuals involved with the recovery activities will need to ensure they will be prepared to respond to a disaster in a concise and coordinated manner.
- What incidents have occurred in the past that tested the recovery capabilities of the IT systems, how plans have been modified as a result of the incidents, and what simulated testing is required to refine the effectiveness of the plan.

Because organizational and operational design variances exist between the 23 campuses and the Office of the Chancellor, each campus process must consider many unique factors. Campuses have been directed to prepare ITDR plans for disasters via multiple directives, including, but not limited to, EO 1014 and ICSUAM §8085.0.

ICSUAM §8085.0, Business Continuity and Disaster Recovery, represents the most recent and specific guidance to campuses in regard to ITDR planning. Simply stated, the policy directs campuses to ensure that information assets can continue to operate or, in a reasonable time frame, be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster or other emergency event. Although the policy itself does not provide detailed operational requirements, it can be surmised that the campuses must consider a multitude of factors such as restart times, backup and recovery procedures, system
security (environmental, physical, and logical), and system interdependence and redundancy to ensure a satisfactory level of continued operational capacity.

At California State University, Bakersfield (CSUB), the campuswide ITDR plan is managed by the campus central IT department, with the assistance of the safety and risk management and university police departments. ITDR was last audited at CSUB during the 2010/11 audit cycle.

SCOPE

We visited the CSUB campus from August 29, 2016, through September 23, 2016. Our audit and evaluation included the audit tests we considered necessary in determining whether operational and administrative controls are in place and operative. The audit focused on procedures in effect from January 1, 2015, through June 30, 2016.

Specifically, we reviewed and tested:

- The administration of the ITDR program to ensure there is a defined mission, stated goals and objectives, clear lines of organizational authority and responsibility, and adequate funding.
- Whether the ITDR plan is reviewed and modified on a regular basis, modifications reflect the needs of the campus and business units, and plans are integrated with the campus business continuity plan.
- Whether the campus business unit’s business impact assessments are considered in determining the prioritization of systems and their recovery time expectations.
- Whether an adequate emergency operations center (EOC) exists; sufficient equipment, supplies, and other critical resources are properly provisioned; and the campus is fully prepared for emergencies affecting data-processing activities.
- The ITDR plan to determine whether it clearly identifies who has authority and responsibility for emergencies and incidents and whether the emergency organization is sufficient to ensure that campus command/incident command techniques provide command and control when emergency incidents occur.
- The adequacy of system redundancy or alternate processes that were developed to ensure minimal interruption of critical business services.
- System backups and record retention to ensure they are sufficient to meet the recovery objectives of the campus.
- Training to ensure that it has been provided to employees, disaster recovery staff, and building marshals who are expected to execute the ITDR plan.
- Whether routinely scheduled simulated tests of plan components are conducted.
• Whether end-user desk procedures define the actions required to adequately synchronize data recovery and restoration efforts.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

Our testing and methodology was designed to provide a managerial-level review of ITDR practices, which included campus policy; governance and risk management; completeness of planning documentation, including replacement equipment contract details and recovery provisions; security and adequacy of data center and alternative site controls; data backup and availability; and manual operating desk procedures. Our testing approach was designed to provide a broad view of controls surrounding ITDR practices.

CRITERIA

Our audit was based upon standards as set forth in California State University Board of Trustee policies; Office of the Chancellor policies, letters, and directives; campus policies and procedures; and other sound administrative practices. This audit was conducted in conformance with the Institute of Internal Auditors’ *International Standards for the Professional Practice of Internal Auditing*.

This review emphasized, but was not limited to, compliance with:

• ICSUAM §8085.0, *Business Continuity and Disaster Recovery*
• EO 1014, *California State University Business Continuity Program*

AUDIT TEAM

Senior Director: Mike Caldera
Audit Manager: Greg Dove
Senior Auditor: Ernesto Pangilinan