February 17, 2017

Dr. Joseph I. Castro, President  
California State University, Fresno  
5241 North Maple Avenue  
Fresno, CA 93740

Dear Dr. Castro:

Subject: Audit Report 16-50, IT Disaster Recovery, California State University, Fresno

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, Fresno

Audit Report 16-50
November 29, 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, controls evaluated were not adequate, appropriate, or 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. We found that the campus ITDR plan contained some of the necessary components, but it was out-of-date, incomplete, and was not available to IT staff or other campus staff who would utilize it during a disaster. In addition, there was a lack of oversight over the plan, and in general, the content was inadequate.

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

1. OVERSIGHT RESPONSIBILITY

OBSERVATION

The responsibility for updating the ITDR plan was unassigned.

Roles, responsibilities, and authorities should be defined and documented, and campus management should appoint a person with appropriate seniority and authority to be accountable for the ITDR plan and implementation.

RECOMMENDATION

We recommend that the campus assign an appropriate staff member the responsibility for updating the ITDR plan.

MANAGEMENT RESPONSE

We concur. The chief information officer has assigned the responsibility for updating the ITDR plan to a designated staff member in technology services by March 1, 2017.

2. ITDR PLAN UPDATES

OBSERVATION

The ITDR plan had not been updated since 2012.

We found that:

- The campus did not maintain a prioritized list of critical IT systems and supporting equipment that would need to be restored in a disaster.

- The disaster recovery plan (DRP) did not include the team member names or the contact information for the recovery teams.

- The IT DRP did not include an estimated timeline for the restoration of core infrastructure, systems, and applications. Additionally, the plan did not consider 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, including the areas noted above.
MANAGEMENT RESPONSE

We concur. The campus will update the ITDR plan in accordance with the areas noted in the recommendation by May 1, 2017.

3. ALTERNATE PROCESSING FACILITY

OBSERVATION
The campus had not identified 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.

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. The campus will identify another California State University campus that has the ability to house and support relocated campus equipment related to campus data centers and will enter into a memorandum of understanding by April 1, 2017.

4. 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.

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

MANAGEMENT RESPONSE
We concur. The campus will identify and contract with an offsite location for storage of physical or digital backup copies of data files by May 1, 2017.
5. **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 emergency equipment and reinforce employee safety and emergency protocol responsibilities in the event of a disaster.

**MANAGEMENT RESPONSE**

We concur. The campus will train data center staff to properly operate data center emergency equipment and will reinforce employee safety and emergency protocol responsibilities in the event of a disaster by March 1, 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. The campus will update its BIAs to include the impact of 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 by May 1, 2017.
7. MANUAL PROCESSING AND LOST DATA PROCEDURES

OBSERVATION

The manual processing procedures created by the campus business departments had not clearly documented specific steps required to continue conducting critical business functions in the event that data processing capabilities were unavailable and did not include instructions about how to re-create lost data.

RECOMMENDATION

We recommend that the campus clearly document the manual desk procedures required to conduct critical business functions in the event data processing services are unavailable and include instructions on how to re-create lost data.

MANAGEMENT RESPONSE

We concur. By May 1, 2017, the campus (i.e., admissions, student accounting, financial aid, accounts payable, etc.) will clearly document the manual desk procedures required to conduct critical business functions in the event data processing services are unavailable. Instructions on how to re-create lost data will be included in these procedures.
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, Executive Order (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, Fresno, the central IT services department manages and maintains the campuswide ITDR program. Additionally, the campus risk management/business continuity department facilitates the completion of the BIAs, a key element needed to prepare the ITDR plan.

SCOPE

We visited the California State University, Fresno campus from July 18, 2016, through August 12, 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