June 5, 2018

Dr. Jeffrey D. Armstrong, President  
California Polytechnic State University, San Luis Obispo  
1 Grand Avenue  
San Luis Obispo, CA 93407  

Dear Dr. Armstrong:

Subject: Audit Report 18-81, IT Disaster Recovery,  
California Polytechnic State University, San Luis Obispo

We have completed an audit of IT Disaster Recovery as part of our 2018 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 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 Polytechnic State University,
San Luis Obispo

Audit Report 18-81
May 2, 2018
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

We found the control environment for some of the areas reviewed to be in need of improvement.

Based upon the results of the work performed within the scope of the audit, except for the weaknesses described below, the operational and administrative controls for ITDR as of March 2, 2018, taken as a whole, provided 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 overall campus business continuity plan. The central information technology services (ITS) ITDR plan at California Polytechnic State University, San Luis Obispo (Cal Poly San Luis Obispo) was out of date, and business impact assessments (BIA) had not been performed for all campus departments that were dependent on the availability of data processing services. In addition, the campuswide ITDR plan did not include a comprehensive test plan; however, the campus had implemented redundant systems and facilities to help mitigate local disasters affecting the central ITS data center and decentralized IT support groups server rooms.

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

1. BUSINESS IMPACT ASSESSMENTS

OBSERVATION

Administration of campus BIAs needed improvement.

We found that:

- BIAs were not reviewed and updated annually.

- The campus had not completed BIAs for some departments to document the business dependence and expectation for recovery, specifying the number of days the department could continue without data processing services before the business operation would be severely impacted.

Executive Order (EO) 1014 requires campuses to review BIAs annually and identify essential business application systems that would need to be restored in the event of a disaster. In addition, BIAs are essential in establishing recovery priorities and a recovery timeline by documenting the length of time data processing services could be disrupted before business activities would be severely impacted.

RECOMMENDATION

We recommend that the campus:

a. Review and update BIAs annually.

b. Complete BIAs for all campus departments to document the business dependence and expectation for recovery, specifying the number of days the department could continue without data processing services before the business operation would be severely impacted.

MANAGEMENT RESPONSE

We concur. The BIA is important to understand the campus prioritization of service restoration. In particular:

a. Risk management will coordinate the update of the campus BIA.

b. Each campus college and division, utilizing the template/BIA application proposed by the campus, will develop their respective BIA.

Estimated completion date: October 1, 2018
2. ITDR PLAN TESTING

OBSERVATION

The campus had not regularly performed comprehensive testing of the ITDR plan to provide support for all of the assumptions in the plan, to verify that vendor and staff contact information was current, and to validate the recovery timeline established.

EO 1014 requires that the campus create a detailed recovery test plan and that all key components of the plan are tested within a seven-year time frame. Additionally, the absence of a current, tested, and easily executable ITDR plan could result in unnecessary financial and non-financial losses in the event of a disaster and create recovery delays outside of management expectations.

RECOMMENDATION

We recommend that the campus perform comprehensive testing of the ITDR plan to provide support for the assumptions in the plan, to verify that vendor and staff contact information is current, and to validate the recovery timeline established.

MANAGEMENT RESPONSE

We concur. In consultation with ITS, the Cal Poly Department of Emergency Management (DEM) and risk management will coordinate comprehensive testing of the ITDR.

Estimated completion date: November 1, 2018

3. ITDR PLAN UPDATES

OBSERVATION

The ITDR plan had not been updated since 2013, and responsibility to ensure that the plan was periodically reviewed, updated, and approved had not been assigned.

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

- A prioritized list of critical IT systems and services establishing the order in which to recover systems during an emergency.
- Clearly defined roles, responsibilities, and authorities for establishing accountability for the ITDR plan and implementation.
- 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. ITS and DEM will coordinate the review and update of disaster recovery plans across campus and develop a testing schedule. In particular:

a. Through the BIA process, a list of critical IT systems and services will be identified with respective recovery order.

b. ITS/DEM/risk management will review campus ITDRs to ensure they clearly define roles, responsibilities, and authorities for campus recovery operations.

c. Utilizing the BIA generated list of critical IT systems and services, we will develop a restoration timeline.

Estimated completion date: October 1, 2018

4. HOSTED SERVICES DOCUMENTATION

OBSERVATION

The campus did not have an up-to-date memorandum of understanding (MOU) with California State University, Monterey Bay (CSUMB) for the IT equipment hosted in its data center, and service level agreements (SLA) were not up to date for the services provided to other campus organizations.

RECOMMENDATION

We recommend that the campus obtain a signed MOU between the campus and CSUMB and signed SLAs between the ITS department and campus organizations that use the ITS facility and services.

MANAGEMENT RESPONSE

We concur. ITS will review current MOU documents on file. We will update MOUs, creating new documents where applicable and ensuring all parties have current files. We will establish a business process to review MOUs on a periodic basis, as defined by campus policy.

Estimated completion date: November 1, 2018
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 Cal Poly San Luis Obispo, the campuswide ITDR plan consists of separate ITDR plans managed by the various campus technical support groups, such as ITS, the administration and finance division, network and technology services, Cal Poly Corporation, and Associated Students, Incorporated, among others. The department of emergency management serves as the lead coordinating department for all campuswide disaster preparedness, response, recovery, and mitigation. In addition, ITS also offers virtual server and physical server hosting services for campus departments at the campus data center. In the event of a disaster, ITS’s responsibility is to restore the core campus technological infrastructure (such as internet and network connectivity, virtual server hardware, and Domain Naming Service), and departments are responsible for restoring their individually owned hardware housed at the data center.

SCOPE

We visited the Cal Poly San Luis Obispo campus from February 5, 2018, through March 2, 2018. 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, 2017, through March 2, 2018.

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

Assistant Vice Chancellor: Mike Caldera
IT Audit Manager: Greg Dove
Senior IT Auditor: Summy Voong