September 26, 2018

Dr. Eduardo M. Ochoa, President
California State University, Monterey Bay
100 Campus Center, Administration Building
Seaside, CA 93955

Dear Dr. Ochoa:

Subject: Audit Report 18-82, IT Disaster Recovery, California State University, Monterey Bay

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 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

Timothy P. White, Chancellor
IT DISASTER RECOVERY

California State University, Monterey Bay

Audit Report 18-82
August 7, 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 operational and administrative 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, except for the weaknesses described below, the operational and administrative controls for ITDR as of June 15, 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 ITDR plan at California State University, Monterey Bay (CSUMB) and the business impact assessments (BIA) were current; however, recovery time expectations and the prioritized list of systems, as determined by IT, had not been clearly communicated to the campus community. Campus departments also had not documented manual procedures required to conduct business in the event that data-processing capabilities were unavailable for an extended period. In addition, the campuswide ITDR plan did not include a comprehensive test plan; however, the campus had implemented data restoration procedures and redundant systems and facilities to help 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. BUSINESS CONTINUITY COORDINATION AND COMMUNICATION

OBSERVATION

Recovery time expectations and the prioritized list of systems, as determined by IT, had not been clearly communicated to the individual business units or campus departments.

Specifically, we noted that information technology services (ITS) had not coordinated with the individual business units to convey that data-processing outages could last for a minimum of five days and manual desk procedures may need to be followed until the systems could be restored.

RECOMMENDATION

We recommend that the campus develop an overall business continuity program to ensure that business expectations are clearly communicated to the IT department, and convey the length of time data-processing outages may last and whether manual desk procedures may need to be followed.

MANAGEMENT RESPONSE

We concur. Risk Management, in coordination with the IT department, will augment our business continuity program (BCP) and ITDR program to ensure communication of business expectations from departments to IT and also ensure communication to departments of projected potential duration of data-processing outages and the possible transition to manual desk procedures.

Expected completion date: January 15, 2019

2. MANUAL PROCESSING DOCUMENTATION

OBSERVATION

Campus departments had not documented manual desk procedures that may be required to conduct business in the event that data-processing capabilities were unavailable for an extended period of time.

RECOMMENDATION

We recommend that the campus clearly document the manual desk procedures required to conduct critical business functions for those departments that use unique systems and applications in the event data-processing services are unavailable for extended periods.
MANAGEMENT RESPONSE

We concur. We will support departments conducting critical business functions that rely on unique systems and applications to document manual desk procedures for implementation when data processing is unavailable for extended periods.

Expected completion date: February 15, 2019

3. BUSINESS CONTINUITY AND DISASTER RECOVERY TEST PLAN

OBSERVATION

The campus had not developed a comprehensive test plan nor performed tests to validate the business continuity and ITDR plan strategy.

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 time frame. Additionally, the absence of a current, tested, and easily executable business continuity and 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 develop a comprehensive test plan of the business continuity and ITDR plans to provide support for assumptions in the plans, and perform tests to validate the established recovery time frame.

MANAGEMENT RESPONSE

We concur. We will create a comprehensive schedule for testing and validating BCP and ITDR assumptions, including recovery time frames.

Expected completion date: January 15, 2019
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 CSUMB, the campuswide ITDR plan is centrally managed by the chief information officer, who oversees all IT departments and resources, including those servicing the University Corporation and Foundation auxiliary organizations. The enterprise risk management and emergency management departments serve as the lead coordinating departments for the campuswide business continuity plan and disaster recovery preparedness, response, and mitigation. ITDR was last audited at CSUMB in 2010.

SCOPe

We visited the CSUMB campus from May 21, 2018, through June 15, 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 June 15, 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

- IT Audit Manager: Greg Dove
- Senior IT Auditor: Summy Voong