The California State University
OFFICE OF THE CHANCELLOR

Audit and Advisory Services
401 Golden Shore
Long Beach, CA 90802-4210

Larry Mandel
Vice Chancellor and
Chief Audit Officer

562-951-4430
562-951-4955 (Fax)
lmandel@calstate.edu

January 10, 2020

Dr. Ellen J. Neufeldt, President
California State University San Marcos
333 S. Twin Oaks Valley Road
San Marcos, CA 92096

Dear Dr. Neufeldt:

Subject: Audit Report 19-86, *IT Disaster Recovery*, California State University San Marcos

We have completed an audit of *IT Disaster Recovery* as part of our 2019 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

c: Timothy P. White, Chancellor

The California State University
Audit and Advisory Services

IT DISASTER RECOVERY

California State University
San Marcos

Audit Report 19-86
November 18, 2019

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, except for the weaknesses described below, the operational and administrative controls for ITDR as of September 13, 2019, 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 campus business continuity plan. California State University San Marcos had an ITDR plan; however, we could not determine whether the plan would satisfy the business recovery requirements because those had not been defined. Business impact assessments (BIA) required by Executive Order (EO) 1014*, California State University Business Continuity Planning Program*, were not current or were missing, and BIAs did not document the business dependence and expectation for recovery of IT services. Also, the ITDR plan did not include a comprehensive test plan, though the campus had implemented redundant systems and facilities to help mitigate potential local disasters that could affect the data center. Further, the campus business units had not documented manual procedures that may be required to conduct ongoing business in the event that data-processing capabilities were unavailable for an extended period, including steps for the recovery and re-creation of any lost data.

Specific observations, recommendations, and management responses are detailed in the remainder of the report.

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. BUSINESS IMPACT ASSESSMENTS

OBSERVATION

The campus had not completed BIAs to document IT dependencies.

We found that:

- The business units had not identified the critical business systems and their recovery time expectations nor communicated the recovery priority and recovery time expectations to instructional and information technology services (IITS).

- Campus business departments had not documented the manual desk procedures that would be used to conduct business in the event that data-processing capabilities were unavailable.

- Campus business departments had not documented the steps that would be taken to identify and re-create lost data, if necessary.

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 complete BIAs to:

a. Document IT dependencies and recovery expectations of the IITS department.

b. Document manual desk procedures that would be used by campus business departments to conduct business in the event that data-processing capabilities were unavailable.

c. Document the steps that will be taken by campus business departments to identify and re-create lost data.

MANAGEMENT RESPONSE

We concur. The campus will complete BIAs to document IT dependencies and recovery expectations and document the manual desk procedures to be used by the campus departments that must conduct business during a disaster or emergency situation.

Estimated completion date: April 1, 2020

2. IT DISASTER RECOVERY PLAN UPDATES

OBSERVATION

The campus ITDR plan requires updating to align with the business requirements in the BIA.

The recovery efforts by the IITS department should be designed to support the recovery needs and priorities defined by the campus through the BIA process.

RECOMMENDATION

We recommend that the campus update the ITDR to align with the business requirements in the BIA.

MANAGEMENT RESPONSE

We concur. The campus will update the ITDR to align with the business requirements in the BIA.

Estimated completion date: May 15, 2020

3. BACKUP DATA

OBSERVATION

The campus backup strategy for critical data needed improvement.

We found that the campus had not provided the IITS department with information regarding which systems were critical to business or departmental operations, and some critical data was not being sent to an offsite storage location. The IITS department maintained two copies of data on campus in separate locations, but the campus business units had not validated the sufficiency of this backup approach or validated that offsite copies of the data are not needed.

Departmental collaboration is needed to ensure that backup copies of data are sufficiently maintained and that recovery strategies align with business requirements.

RECOMMENDATION

We recommend that the campus evaluate the backup strategy of critical data and determine whether additional copies of critical data should be stored in an offsite location.

MANAGEMENT RESPONSE

We concur. The campus will evaluate the backup strategy of critical data and determine whether additional copies of critical data should be stored in an offsite location.

Estimated completion date: May 15, 2020

4. DISASTER RECOVERY TEST PLAN

OBSERVATION

The campus had not developed a comprehensive ITDR test plan or performed tests to validate the ITDR plan strategy.

EO 1014, *California State University Business Continuity Program,* requires the campus to create a detailed recovery test plan and test all key components of the plan within a seven-year time frame.

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 could create recovery delays outside of management expectations.

RECOMMENDATION

We recommend that the campus develop a comprehensive ITDR test plan and perform tests to validate the ITDR plan strategy.

MANAGEMENT RESPONSE

We concur. The campus will develop a comprehensive ITDR test plan and perform tests to validate the ITDR plan strategy.

Estimated completion date: May 15, 2020

GENERAL INFORMATION

BACKGROUND

ITDR planning is a specific subset of the campus business continuity planning (BCP) 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, *California State University Business Continuity Program,* and ICSUAM §8085.0, *Business Continuity and Disaster Recovery*.

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 San Marcos, the campuswide ITDR plan includes many disaster scenarios that the campus believes to be most relevant. This plan is developed and updated by the IITS group. Many of the computing resources are not hosted on campus and are leveraging third-party vendors and cloud-based systems. IITS is responsible for the recovery of the data centers on campus in the event of a disaster, including network connectivity, servers, software, and data. IITS has leveraged redundancy to provide availability of IT resources to the campus and maintains backup copies of data at a separate on-campus location.

SCOPE

We visited the California State University San Marcos campus from August 19, 2019, through September 13, 2019. 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 July 1, 2019, through September 13, 2019.

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
IT Auditor: Christopher Burk