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*

April 9, 2020

Dr. Leroy M. Morishita, President
California State University, East Bay
25800 Carlos Bee Boulevard
Hayward, CA 94542

Dear Dr. Morishita:

**Subject: Audit Report 19-88, *IT Disaster Recovery*, California State University, East Bay**

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, East Bay

Audit Report 19-88
February 26, 2020

# 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 January 9, 2020, taken as a whole, provided reasonable assurance that risks were being managed and objectives were met.

ITDR plans are a key component to ensure that an organization is prepared to restore IT systems in the event of a disaster. At California State University, East Bay, the campus was in the process of updating its ITDR plan to reflect the current landscape of its IT systems, which are mostly cloud-based. However, the draft plan was missing some components to ensure a timely and effective recovery, including an ITDR test plan.

Additionally, the campus did not have recovery teams defined for the components of their campus recovery. A recovery team is an important portion of the ITDR plan to ensure that the components of the plan are assigned and the staff is prepared to fulfill its role in the recovery efforts. We also noted that the campus' emergency operations center was missing some key components to ensure that the facility could be used in an emergency, including a backup power source for the operations of the EOC and a staff roster to contact key campus leaders regarding the status of the recovery. Further, we noticed that the staff had not been trained in emergency procedures for the data center. Though the staff does not typically work out of the data center, staff members should be trained in the emergency features of the room to ensure that when they need to facilitate work out of the data center, they will be prepared to operate the emergency equipment, including the gas fire suppression system.

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

# OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

## 1. ITDR PLAN COMPONENTS

**OBSERVATION**

The campus had not completed a comprehensive ITDR plan.

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

- An ITDR test plan.
- A detailed list of recovery teams, along with members and their roles and responsibilities.
- A reasonable recovery timeline that incorporates IT capabilities and business requirements as defined in the BIAs.

**RECOMMENDATION**

We recommend that the campus:

a. Create an ITDR test plan for IT recovery capabilities with each component tested at least once every seven years.

b. Define recovery teams with detailed roles and responsibilities assigned to each member.

c. Define practical and acceptable recovery timelines that incorporate IT capabilities and business requirements defined in the business impact assessments (BIAs).

**MANAGEMENT RESPONSE**

We concur. These updates to the campus ITDR plan will be completed by August 31, 2020:

a. A test plan for IT recovery capabilities, including the testing of identified components at least once every seven years.

b. Defined recovery teams with detailed roles and responsibilities assigned to each member.

c. Defined recovery timelines that incorporate IT capabilities and business requirements as defined in the BIAs.

## 2. IT DISASTER RECOVERY PLAN UPDATE

**OBSERVATION**

The ITDR plan had not been updated since 2013 and was in the process of being updated during our audit.

Specifically, we found that the current plan did not include the current technologies used by the campus.

**RECOMMENDATION**

We recommend that the campus finish updating the ITDR plan.

**MANAGEMENT RESPONSE**

We concur. The ITDR plan will be updated by August 31, 2020, and will include the current technologies used by the campus.

## 3. EMERGENCY OPERATIONS CENTER

**OBSERVATION**

The campus emergency operations center (EOC) did not have some components that would be needed during data processing recovery efforts.

Specifically, the campus did not have a backup power supply to run EOC operations, and a copy of the staff roster that would be used to contact key campus leaders regarding the status of the recovery was not kept onsite.

The campus had recently moved to a new EOC. Availability of emergency power and local access to notification lists helps ensure that the EOC can operate with minimal dependence on the availability of other resources.

**RECOMMENDATION**

We recommend that the campus update the EOC to include:

a. A backup power supply to run EOC operations.
b. A local copy of the staff roster of key campus leaders.

**MANAGEMENT RESPONSE**

We concur. The EOC will be updated as follows:

a. A backup power supply to run EOC operations will be added by May 31, 2020.

b. A copy of the staff roster of key campus leaders will be maintained onsite by April 30, 2020.

## 4. INFORMATION TECHNOLOGY EMERGENCY TRAINING

**OBSERVATION**

The campus had not trained all data center staff to properly operate emergency equipment in the data center.

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 emergency equipment in the data center.

**MANAGEMENT RESPONSE**

We concur. The current data center staff will be trained by June 30, 2020, on how to properly operate emergency equipment in the Hayward data center.

# 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, 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, East Bay (CSUEB), the campus ITDR plan was in the process of being updated during our audit by the IT department, who will maintain and update the ITDR plan. Many of the computing resources are not hosted on campus and are leveraging third-party vendors and cloud-based systems. Accordingly, their recovery efforts will focus on ensuring access to resources stored in the cloud. In addition, the IT department has implemented many redundant systems to help ensure continued availability of IT resources to the campus.

## SCOPE

We visited the CSUEB campus from December 2, 2019, through January 9, 2020. 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 February 15, 2013, through January 9, 2020.

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