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 15, 2020

RADM Thomas A. Cropper, President
California State University Maritime Academy
200 Maritime Academy Drive
Vallejo, CA 94590

Dear Admiral Cropper:

Subject: Audit Report 19-87, *IT Disaster Recovery*, California State University Maritime Academy

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
Maritime Academy

Audit Report 19-87
March 5, 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 December 19, 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. We found that the California State University Maritime Academy plan and alternative processing location needs improvement to ensure timely recovery of critical IT services. Before the start of our review, the campus experienced a major fire that disrupted the operations of the entire campus, and data processing services were not restored timely. In addition, campus departments and business units were in the process of documenting business impact assessments (BIA) but had not yet completed them.

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

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. ITDR PLAN

OBSERVATION

The campus ITDR plan did not have sufficient detail for the campus to be able to timely recover critical IT services.

We noted that:

- The training ship Golden Bear (TSGB) was defined in the plan as the alternate processing facility; however, the TSGB can provide only limited recovery services due to its location, availability, and technical capabilities. The plan did not define alternative sites that could provide full or partial recovery services.

- The plan did not include a strategy for replacing damaged equipment, and the campus did not have an inventory of replacement equipment needed to support critical IT services.

- The campus did not have a defined and documented escalation plan beyond designating the chief information officer (CIO) as the person responsible for declaring a disaster and activating the plan. Additionally, the plan did not include a list of campus leadership personnel to be notified in the event of a declared disaster.

The lack of an adequate alternative processing facility, equipment replacement strategy and inventory of equipment needs, and proper escalation and notification plans could result in miscommunication, delayed activation of the plan, incomplete or limited recovery of critical IT services, and interruption of operations.

RECOMMENDATION

We recommend that the campus perform a full review of ITDR capabilities and subsequently design and document a new recovery plan and strategy that:

a. Identifies a suitable alternative processing facility that can provide full recovery services or provides a plan for the campus to transition to cloud-based services.

b. Identifies a strategy for replacing damaged equipment and developing an inventory of replacement equipment needed to support critical IT services, or provides a plan for the campus to transition to a cloud-based recovery strategy.

c. Develops an escalation and notification plan that identifies who can activate the plan in the event of the CIO's absence and which campus leadership personnel are to be notified in the event of a disaster.

MANAGEMENT RESPONSE

The campus will perform a full review of ITDR capabilities and design and document a new recovery plan and strategy that includes a plan for the campus to transition critical services to cloud-based services. The plan will include an escalation and notification plan that identifies who can activate the plan in the event of the CIO's absence and which campus leadership personnel are to be notified in the event of a disaster.

Estimated completion date: June 30, 2020

2. BUSINESS IMPACT ASSESSMENTS AND MANUAL PROCESSING PROCEDURES

OBSERVATION

The campus did not have a process to complete and document BIAs that identified and prioritized dependencies on critical IT services, applications, and subsequent recovery time objectives.

Additionally, campus departments and business units had not defined and documented manual processing procedures, including procedures addressing a potential data loss, in the event IT services and applications are unavailable.

The lack of completed BIAs, including manual processing and data loss procedures, may result in delayed recovery and interruption of operations.

RECOMMENDATION

We recommend that the campus:

a. Identify the dependencies on data processing services by completing BIAs for all departments and business units, and communicate the results to IT as a basis for disaster recovery planning.

b. Define and document manual processing and data loss procedures for campus departments and business units as part of the BIAs.

c. Implement a process to ensure that all campus departments and business units review and update BIAs annually.

MANAGEMENT RESPONSE

The campus will complete and annually review BIAs for all departments and business units that identify the data processing service dependencies. The results will be used as a basis for disaster recovery planning, including manual processing and data loss procedures for campus departments.

Estimated completion date: July 30, 2020

3. DATA CENTER PHYSICAL SECURITY

OBSERVATION

The campus data center used to house the classroom simulator equipment did not have door-locking mechanisms that record individual entry and accountability, and the dual-purpose facility did not include properly locking equipment cages to protect the campus IT department equipment.

Without physical access traceability and secured equipment cages, critical equipment may be tampered with and unauthorized or malicious activities would not be detected.

RECOMMENDATION

We recommend that the campus implement a physical access control mechanism via video cameras or a badging system with audit trail logging, and that IT-owned equipment cages be secured with lock and key.

MANAGEMENT RESPONSE

The campus will implement a physical access control mechanism via video cameras or a badging system with audit trail logging, and IT-owned equipment cages will be secured with lock and key.

Estimated completion date: June 30, 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, 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 Maritime Academy, the IT department manages and maintains the ITDR plan. The IT department does not host any computing equipment for auxiliary organizations, although auxiliary organizations consume common shared IT services. Business continuity planning falls under the department of safety and risk management within the office of Administration and Finance.

SCOPE

We visited the California State University Maritime Academy campus from December 2, 2019, through December 19, 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 January 1, 2019, through December 19, 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
Senior IT Auditor: Clement Chen