October 10, 2018

Dr. Judy K. Sakaki, President
Sonoma State University
1801 E. Cotati Avenue
Rohnert Park, CA 94928

Dear Dr. Sakaki:

Subject: Audit Report 18-83, IT Disaster Recovery, Sonoma State University

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

c: Timothy P. White, Chancellor
IT DISASTER RECOVERY

Sonoma State University

Audit Report 18-83
August 27, 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

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

Based upon the results of the work performed within the scope of the audit, the operational and administrative controls for ITDR as of June 16, 2018, were unlikely to provide reasonable assurance that risks were being managed and objectives were met. The campus had no discernable current plan for the recovery of data processing services.

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 Sonoma State University (SSU) ITDR plan was out-of-date and had not been updated since 2005. Critical system and equipment listings and contact information was also outdated, recovery facilities had not been identified, and recovery procedures were not documented. In addition, business impact assessments had not been documented by all departments on campus.

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

1. ITDR PLAN UPDATES

OBSERVATION

The ITDR plan had not been updated since 2005, and the responsibility to ensure that the plan was periodically updated, reviewed, and approved had not been assigned.

In addition, the plan did not include:

- A listing of campus departments and the applications that would have to be restored in the event of a disaster.
- An updated listing of critical equipment and systems that would need to be recovered after an emergency or disaster.
- An updated 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.
- A detailed list of recovery teams, along with names of team members and their roles and responsibilities.

RECOMMENDATION

We recommend that the campus:

a. Update the ITDR plan to include all key elements, including those listed above.
b. Assign responsibility for ITDR plan maintenance to an appropriate staff member.

MANAGEMENT RESPONSE

We concur. The campus will update the ITDR plan to include all key elements, including those listed above. The campus will assign responsibility for the ITDR plan maintenance. We intend to implement the new process by February 28, 2019.

2. ITDR PLAN TESTING

OBSERVATION

The campus had not performed 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 that had been established.
RECOMMENDATION

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

MANAGEMENT RESPONSE

We concur. The campus will perform comprehensive testing of the ITDR plan to provide support for the assumptions of the plan, to verify that vendor and staff contact information is current and correct, and to validate that the recovery timeline is feasible. We intend to implement the new process by February 28, 2019.

3. ALTERNATIVE PROCESSING FACILITY

OBSERVATION

The campus had not identified an off-campus alternative processing facility or another campus that would be able to house and support relocated equipment in the event that campus data centers were adversely impacted by a disaster.

RECOMMENDATION

We recommend that the campus identify an off-campus alternative processing facility or another campus that would be able to house and support relocated campus equipment in the event campus data centers were unavailable due to a disaster.

MANAGEMENT RESPONSE

We concur. The campus will identify an off-campus alternative processing facility or another campus that would be able to house and support relocated campus equipment in the event campus data centers are unavailable due to a disaster. We intend to implement the new process by February 28, 2019.

4. EQUIPMENT REPLACEMENT CONTRACT

OBSERVATION

The campus had not provided the vendor that was under contract to replace equipment in an emergency with an updated listing of critical IT equipment that would need to be replaced in a disaster.

Without providing a current listing of equipment to the vendor, the campus could experience a delay in the delivery and restoration of critical infrastructure equipment.
RECOMMENDATION

We recommend that the campus implement a process to update and maintain the listing of critical IT equipment that would need to be replaced in a disaster, and provide it to the vendor under contract to replace equipment in an emergency.

MANAGEMENT RESPONSE

We concur. The campus will implement a process to update and maintain the listing of critical IT equipment that may need to be replaced in a disaster. This listing will be provided to the vendor under contract to replace equipment in an emergency. We intend to implement the new process by February 28, 2019.

5. BUSINESS IMPACT ASSESSMENTS

OBSERVATION

The campus did not ensure that each department had completed a business impact assessment (BIA) and did not have a process to review and approve BIAs annually.

We found that only three campus departments had completed BIAs.

Executive Order 1014 requires campuses to review BIAs annually and identify essential business applications that would need to be restored in the event of a disaster. In addition, BIAs are essential in establishing 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. Implement a process to ensure that all campus departments complete BIAs.

b. Review and update BIAs annually.

MANAGEMENT RESPONSE

We concur. The campus will implement a process to ensure that all campus departments complete BIAs and that those BIAs are updated and reviewed annually. We intend to implement the new process by February 28, 2019.

6. HOSTED SERVICES DOCUMENTATION

OBSERVATION

The campus did not have an up-to-date memorandum of understanding (MOU) with two campus auxiliary organizations, Sonoma State University Foundation and Sonoma State
Enterprises, Inc., documenting the roles and responsibilities for hosting services provided to the auxiliary organizations.

**RECOMMENDATION**

We recommend that the campus create an up-to-date MOU to document the roles and responsibilities for the hosting services provided to auxiliary organizations.

**MANAGEMENT RESPONSE**

We concur. The campus will create an up-to-date MOU to document the roles and responsibilities for the hosting services provided to auxiliary organizations. We intend to implement the new process by February 28, 2019.

7. **IT STAFF EMERGENCY TRAINING**

**OBSERVATION**

The campus had not documented the completion status of IT emergency training for the employees who worked at the Schulz data center.

**RECOMMENDATION**

We recommend that the campus maintain IT emergency training completion documentation for the employees who work at the Schulz data center.

**MANAGEMENT RESPONSE**

We concur. The campus will maintain completed IT emergency training documentation for the employees who work at the Schulz data center. We intend to implement the new process by February 28, 2019.

8. **MANUAL PROCESSING PROCEDURES**

**OBSERVATION**

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

Additionally, the campus had not documented the procedures necessary to re-create lost data in the event of a disaster.

**RECOMMENDATION**

We recommend that the campus departments document the manual steps needed to conduct business in the event that data-processing capabilities were unavailable, and include procedures for the re-creation and data entry of any lost data.
MANAGEMENT RESPONSE

We concur. The campus will document the manual steps needed to conduct departmental business in the event that data-processing capabilities become unavailable. This includes procedures for the re-creation and data entry of any lost data. We intend to implement the new process by February 28, 2019.

9. BACKUP DOCUMENTATION

OBSERVATION

The campus had not documented the procedures necessary to recover data from the vendor-hosted cloud backup storage platform.

In addition, the campus was not retaining a copy of the ITDR plan offsite.

RECOMMENDATION

We recommend that the campus create comprehensive instructions to recover data from the vendor-hosted cloud backup storage platform and retain a copy of the ITDR plan offsite.

MANAGEMENT RESPONSE

We concur. The campus will create comprehensive instructions to recover data from the vendor-hosted cloud backup storage platform and retain a copy of the ITDR plan offsite. We intend to implement the new process by February 28, 2019.

10. FIRE-SUPPRESSION SYSTEM MAINTENANCE

OBSERVATION

The campus had not performed regular maintenance of the Schulz data center fire-suppression system. The system was last inspected in 2015.

RECOMMENDATION

We recommend that the campus inspect the Schulz data center fire-suppression system on a regular basis.

MANAGEMENT RESPONSE

We concur. The campus will begin to inspect the Schulz data center fire-suppression system on a regular basis. We intend to implement the new process by October 31, 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, 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 SSU, the IT department manages and maintains the campuswide ITDR plan. The IT department also hosts the computing equipment for the auxiliary organizations in the campus data center. The risk management department is responsible for maintaining campus departments BIAs, which are needed to create the ITDR plan.

SCOPE

We visited the SSU 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: Ernesto Pangilinan