UC MERCED AUDIT AND ADVISORY SERVICES

August 20, 2015

To: Tom Peterson – Executive Vice Chancellor and Provost

Subject: Audit of IT Disaster Recovery Planning

Ref: Report No. M15A007

Internal Audit has completed an audit of IT disaster recovery planning at UC Merced, which was part of the Fiscal Year 2014 – 2015 Audit Plan. IT Leadership has put together management corrective actions for the issues identified. We will follow up to verify that management corrective actions are completed.

We appreciate the help we received from the staff of Central IT and the various department system administrators we met with during this audit.

Todd Kucker

Todd Kucker
Internal Audit Director

Attachment

cc: SVP Vacca
Chancellor Leland
Associate Chancellor Putney
Vice Chancellor Reese
Associate Vice Chancellor and Chief Information Officer Kovalchick
Assistant Vice Chancellor Vasquez
Risk Manager Castillo
Dean Meza
Assistant Dean Garcia
Chief Information Security Officer Dugan

UNIVERSITY OF CALIFORNIA, MERCED
AUDIT AND ADVISORY SERVICES

IT Disaster Recovery Planning
Report No. M15A007

August 20, 2015

Work Performed by:
Todd Kucker, Internal Audit Director

Management Summary

Internal Audit has completed an audit of Information Technology Disaster Recovery Planning at UC Merced. The purpose of the audit was to review UC Merced's current disaster recovery planning and to recommend potential improvements.

To review current planning, we discussed procedures with IT employees from Central IT and various IT employees from the different departments and schools to review planning that has been completed.

From our audit, we determined that sufficient IT planning for disasters and other disruptions has not been completed at UC Merced. Overall, the recommendations and guidelines outlined in UC Policy for IT disaster recovery planning have not been implemented. As a result, the risk that campus operations could not quickly recover from a disruption has not been adequately managed and mitigated.

The following report discusses the issues identified, recommendations for implementing IT disaster recovery planning, and management's planned approach for putting together and testing the plan. The recommendations and corrective actions are categorized in the following areas:

- Campus Leadership Support and Sponsorship
- Formal Risk Assessment and Business Impact Analysis
- Disaster Recovery Strategy and Formal Plan
- Testing and Plan Maintenance

Purpose and Scope

Internal Audit has completed an audit of Information Technology Disaster Recovery Planning, which was part of the Fiscal Year 2014 – 2015 audit plan. A disaster recovery plan refers to the plans in place to restore essential Information Technology systems and applications that enable critical business processes. The purpose of the audit was to review UC Merced's current disaster recovery planning and to recommend potential improvements.

To review current planning, we discussed procedures with IT employees from Central IT and various IT employees from the different departments and schools to review planning that has been completed. We met with employees from the following areas:

- Central IT (IT responsibilities under the direct authority of the campus Chief Information Officer)
- Research Computing
- Library
- CatCard (the campus card system managed within Student Affairs)
- School of Natural Sciences
- Housing

While Central IT manages the campus network and infrastructure utilized by all areas of campus, the other IT areas reviewed manage systems and data for their own departments and schools.

Overview of IT Disaster Recovery Planning Requirements

IT controls frameworks stress the need for formal disaster recovery planning. UC Policy BFB-IS-12 *Continuity Planning and Disaster Recovery* explains that “the University is committed to actions that will make campus environments safer and more secure as well as less vulnerable and more resilient in the aftermath of catastrophic disaster or other extraordinary disruption.”

BFB-IS-12 provides recommendations and guidelines for information technology continuity planning and disaster recovery planning in support of the University’s commitment to protection of and accessibility to information resources.

The overall goal of continuity planning should be to reduce risk and minimize disruption of campus research and academic programs and of supporting campus business functions. BFB-IS-12 is an overview of the different steps of Disaster Recovery Planning. The following information is a summary of the policy and includes information important to this review.

Risk Assessment (Business Impact Analysis)

Risk assessments or business impact analyses should be conducted to identify all critical functions of the organization or units and their supporting information systems. The impact of loss or disruption of functions should be identified, evaluated, and categorized according to the time frames required for recovery of each function.

Continuity planning should identify, analyze, and prioritize mission-critical functions based on:

- Criticality
- Scope and consequences of disruption
- Survivability (time sensitivity)
- Coordination requirements with other units or external partners
- Facilities, infrastructure, and IT support requirements

Priorities for response and recovery of academic and business systems should be based on a set of principles defined by the unit or department in conformance with its mission critical objectives.

Business and Financial Bulletin IS-3 *Electronic Information Security* requires that risk assessments be conducted and include an inventory of all information resources. All resources should be classified into one of the following categories:

- **Essential** to the continuing operation of the University
- **Necessary** to perform important functions
- **Deferrable** for an extended period of time

Continuity Planning Steps

Continuity planning consists of four overlapping phases – mitigation, preparedness, response, and recovery.

1. Mitigation

Mitigation are the measures put into place to ensure the protection and availability of IT resources. These measures include the steps taken to build redundancy into systems and setting up adequate backup procedures. Essential computing and networking systems must be located in secure, professionally managed data centers that include system and data back up at a secure, off-site locations that provide standard protection against common hazards, such as fire, flood, earthquake, theft, and decay.

2. Preparedness

Preparedness involves the actions required to establish and maintain a level of capability necessary to implement emergency response plans and conduct disaster recovery operations. Preparedness is implemented through a continual cycle of planning, training and equipping, exercising, and evaluating and taking actions to correct deficiencies and mitigate vulnerabilities. Disaster recovery plans should be tested on a periodic basis by various means, such as disaster recovery exercises, testing of alternate sites, or other simulations of potentially predictable emergencies. Plans should be updated to reflect changing environments, processes, technology or other impacts as appropriate.

In general, response and recovery plans should include:

- Identification of responsible authority to direct emergency response
- Communication plans, in conformance with campuswide communication planning strategies
- Communication alternatives to enable community members to communicate with each other and campus personnel
- Inventory and classification of resources
- Emergency response procedures, including the specification of teams of personnel assigned responsibility for responding in emergency situations. Planning should anticipate alternative deployment of personnel to address inability of assigned personnel to participate in response efforts
- Communication alternatives to enable team members to communicate with each other and with management during an emergency
- Provisions for equivalent alternate processing in the event of a disaster or other interruption that renders normal processing inoperable
- Provisions for remote worksites
- Deployment procedures to relocate or replicate resources or facilities
- Procedures that ensure authorized access to back up sites
- Measures to protect vital records or essential data
- Provisions in contracts with external service providers that ensure their preparedness for emergency response and business recovery

3. Response

Response efforts should follow the pre-planned Disaster Recovery Plans. Continuity planning should have determined the priority of activities to address both immediate and longer-term effects of the emergency, including recommended procedures and checklists for action.

4. Recovery

The focus of recovery efforts should be on re-establishing operational capability as identified in planning priorities.

Observations and Conclusion

From our audit, we determined that sufficient IT planning for disasters and other disruptions has not been completed at UC Merced. Overall, the recommendations and guidelines outlined in the UC Policy for IT disaster recovery planning have not been implemented. As a result, the risk that campus operations could not quickly recover from a disruption has not been adequately managed and mitigated.

Central IT and departmental system administrators have identified critical systems and focused on setting up redundancy and backup procedures for systems and data. While this is crucial to building resilience in daily IT operations, the campus should be better prepared for disasters and other disruptions.

It is very important for IT disaster recovery planning to be completed as part of the overall business continuity planning to ensure alignment between business recovery and IT recovery. UC Risk Services manages the UC Ready IT system which manages business (mission) continuity plans. Recently, UC Risk Services implemented enhancements to the UC Ready system which included the ability to conduct a Business Impact Analysis in order to identify the most critical functions and time sensitive processes.

In the past, UC Merced Risk Services has worked with campus departments to monitor whether business continuity plans are up-to-date. Risk Services was recently part of a campus reorganization and moved under the new Assistant Vice Chancellor of Campus Safety. As additional responsibilities have been assigned to Risk Services' limited staff, additional resources will be needed to be identified to adequately manage business continuity planning.

IT disaster recovery planning needs a “champion” from the Campus Safety area to complete the overall business continuity to effectively design and test a Disaster Recovery plan. As Central IT manages many of the critical systems, we recommend that Central IT collaborate with the many IT groups on campus to put together plans and to test the plans. As different departments are involved, this will require the support of campus leadership.

Our recommendations for implementing IT Disaster Recovery planning are categorized in the following areas:

- Campus Leadership Support and Sponsorship
- Formal Risk Assessment and Business Impact Analysis
- Disaster Recovery Strategy and Formal Plan
- Testing and Plan Maintenance

Recommendations and Management Corrective Actions

1. Campus Leadership Support and Sponsorship

Ultimately, the goal of IT disaster recovery planning is to re-establish the operational capability of the campus. As priorities established during planning are business decisions, campus leadership should provide feedback and approve the plans. IT disaster recovery planning should not be viewed as only an IT responsibility. As IT systems at UC Merced are distributed among many different departments, support from campus leadership is essential to the planning.

The IT Advisory Committee (ITAC) should provide oversight for managing the IT disaster recovery plan. The committee should reflect broad representation from campus. Funding should be budgeted for the planning efforts and approved by the IT Advisory Committee.

Management Corrective Action

IT Leadership will submit a multi-year budget to address IT disaster recovery plans based upon the outcome of a formal risk assessment and BIA by March 2016.

2. Formal Risk Assessment and Business Impact Analysis

With the recent reorganization of Risk Services and Campus Safety, the responsibility for monitoring and updating business continuity plans should be assigned to an employee or department within the new Campus Safety area. A campus-wide Business Impact Analysis (BIA) should be conducted under the oversight of this employee or department and include IT's identification and prioritization of credible threats for risk mitigation. Legal, regulatory, financial and operational impacts of a disruption should be analyzed and recovery objectives should be appropriately determined. A business impact analysis (BIA) should address the period of time that systems and functions need to be recovered after a disruption ("Recovery Time Objective") and the point in time in which systems and data must be recovered after a disruption ("Recovery Point Objective").

Management Corrective Action

Pending Vice Chancellor decisions regarding Business Continuity ownership, IT Leadership will work with this employee or department to evaluate the Business Impact Analysis and will provide a list of current RTO and RPO to the Vice Chancellors for review by November 15, 2015.

3. Disaster Recovery Strategy and Formal Plan

After a business impact analysis has been completed and approved by campus leadership, a formal, written disaster recovery plan should be put together that balances IT investment and IT recovery objectives.

A formal disaster recovery plan should be put together and implemented. As part of the plan, standard documentation should be available consisting of response and recovery procedures.

The plan should include the following:

- Response and recovery team responsibilities
- Facility and resource requirements
- Recovery procedures
- A crisis management team should be identified and trained
- Procedures for communicating with employees and vendors should be identified and actionable
- The plans should address technology infrastructure, including recovery of critical IT applications and network assets (voice and data)

The end result should be integrated recovery plan documentation that has been properly distributed and contains the necessary detail to recover from an interruption within the pre-defined recovery time objective.

Management Corrective Action

IT Leadership will begin monthly table-top planning starting in October 2015 to define the items listed above and incorporate BIA objectives approved by the IT Advisory Committee and the Vice Chancellors and present a draft plan by May 2016.

4. Testing and Plan Maintenance

Testing and plan maintenance involves validating existing capabilities to respond to disruptions by exercising the ability to recover and restore operations.

After a formal disaster recovery plan has been implemented, the plan needs to be tested. There should be a testing schedule. Issues noted during testing should be properly documented and subsequently assigned to appropriate employees for resolution. Based upon the issues identified, the plan should be regularly updated.

It is important to test IT disaster recovery plans for all critical systems. Different levels of testing the plans include full testing, table-top exercises, and testing emergency communications information. The tests should include scenarios that mimic actual recovery processes.

Management Corrective Action

IT will complete an IT Disaster Recovery test plan and conduct a table top test of that plan by May 2016.

Other issue identified during the audit

5. Backups not maintained off-site

During our discussions with department system administrators, we noted an instance where backups are not maintained off-site. Research Computing works with the academic units to provide IT resources for storing faculty intellectual property and research funded by grants. The backups are currently maintained in the same data center as the original data. The system administrator mentioned current plans to move backups to another location on campus.

We recommend that backups be maintained further away from the original data. While moving backups to an adjacent campus building will decrease the risk that an incident involving the data center will not destroy the original data and the backups, increasing the distance between the original data and backup would better protect the data.

Management Corrective Action

The Research Computing system administrator recently left UC Merced. While in the past, Research Computing resided in the schools, Central IT will recruit a new system administrator and the Research Computing function will be moved to Central IT.

Central IT will provide and disseminate standards for data backup for data generated by externally funded research by January 2016.

IT will provide service description for off-site data storage for use by faculty research data by January 2016.