IT DISASTER RECOVERY

CALIFORNIA STATE UNIVERSITY,
SACRAMENTO

Audit Report 11-31
September 14, 2011

Members, Committee on Audit

Henry Mendoza, Chair
Melinda Guzman, Vice Chair
Margaret Fortune  Steven M. Glazer
William Hauck  Hsing Kung  Linda Lang

Staff

University Auditor:  Larry Mandel
Interim Senior Director:  Mike Caldera
Audit Manager:  Greg Dove
Senior Auditor:  Gordon Eng

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
## CONTENTS

Executive Summary ................................................................................................................................. 1

Introduction ................................................................................................................................................ 3
  Background .......................................................................................................................................... 3
  Purpose ............................................................................................................................................. 5
  Scope and Methodology ...................................................................................................................... 7

### OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Alternate Processing .................................................................................................................................. 8

Business Continuity and Impact Assessments .......................................................................................... 8

End-User Coordination and Restoration Procedures ................................................................................. 10

Disaster Recovery Planning ..................................................................................................................... 11
  Written Disaster Recovery Plan ........................................................................................................ 11
  Disaster Recovery Plan Testing .......................................................................................................... 13
APPENDICES

APPENDIX A: Personnel Contacted
APPENDIX B: Campus Response
APPENDIX C: Chancellor’s Acceptance

ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CSU</td>
<td>California State University</td>
</tr>
<tr>
<td>EO</td>
<td>Executive Order</td>
</tr>
<tr>
<td>EOC</td>
<td>Emergency Operations Center(s)</td>
</tr>
<tr>
<td>FISMA</td>
<td>Financial Integrity and State Manager’s Accountability Act</td>
</tr>
<tr>
<td>ICSUAM</td>
<td>Integrated California State University Administrative Manual</td>
</tr>
<tr>
<td>IRT</td>
<td>Information Resources and Technology</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITDR</td>
<td>Information Technology Disaster Recovery</td>
</tr>
<tr>
<td>LTAP</td>
<td>Long Term Alternative Processing</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>SAM</td>
<td>State Administrative Manual</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2010, the Board of Trustees, at its January 2011 meeting, directed that Information Technology Disaster Recovery (ITDR) continue to be reviewed. The Office of the University Auditor had previously reviewed ITDR for financial systems in the biennial Financial Integrity and State Manager’s Accountability Act (FISMA) and Auxiliary Organization audits.

We visited the California State University, Sacramento campus from May 9, 2011, through May 20, 2011, and audited the procedures in effect at that time.

Our study and evaluation revealed certain conditions that, in our opinion, would result in significant risk exposures if not corrected. Specifically, the campus did not maintain adequate internal control over the following areas: alternate processing, business impact assessment, disaster recovery plan, and disaster recovery test plans. These conditions, along with other weaknesses, are described in the executive summary and body of this report. In our opinion, due to the effect of the weaknesses described above, the operational and administrative controls for ITDR activities in effect as of May 20, 2011, taken as a whole, were not sufficient to meet the objectives stated in the “Purpose” section of this report.

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.

The following summary provides management with an overview of conditions requiring attention. Areas of review not mentioned in this section were found to be satisfactory. Numbers in brackets [ ] refer to page numbers in the report.

ALTERNATE PROCESSING [8]

The memorandum of understanding between the campus and its designated long-term alternative processing site had not been formalized.

BUSINESS CONTINUITY AND IMPACT ASSESSMENT [8]

The campus process for updating and reviewing business continuity plans (BCP) needed improvement. Specifically, several departmental BCPs had not been updated or reviewed on an annual basis, and some departmental BCPs, including the information technology (IT) plan, were not included in the campus BCP.

END-USER COORDINATION AND RESTORATION PROCEDURES [10]

Coordination between IT and business unit end-users needed improvement. For example, IT had not been informed of the various business units’ recovery expectations as documented in the business impact
analysis, and the potential of losing one weeks’ worth of data had not been communicated to the business units.

DISASTER RECOVERY PLANNING [11]

The written ITDR plan needed improvement; for example, the plan did not include all current systems and proper cross-references to other campus response plans that would be pertinent to a systematic recovery of data processing capabilities. In addition, the campus had not designed a comprehensive plan to test the recovery plan strategies.
INTRODUCTION

BACKGROUND

Information Technology Disaster Recovery (ITDR) planning is a specific subset of an entity’s 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, State Administrative Manual (SAM) §5355-5355.2, Executive Order (EO) 1014, and the Integrated California State University Administrative Manual (ICSUAM) §8085.0.

SAM §5355-5355.2 directs state agencies to develop, implement, test, and modify disaster recovery plans, including plans specific to IT assets. SAM §5355 states that agencies must take appropriate steps to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure that essential business functions will continue in the event of a disaster. SAM §5355.1 states that, in developing an ITDR plan, agencies should provide for the continuity of computing operations in support of critical business functions, minimize the need for decision-making during a disaster and subsequent recovery, and plan for the migration of computing resources toward resumption of operational capacity in an expeditious and efficient manner. In preparing such a plan, SAM §5355.1 directs that ongoing testing, analysis, and modification of plan assumptions and activities must occur. SAM §5355.2 states that each
agency must maintain a list of computer applications that are critical to agency operations, information assets required by such applications, and a method by which such applications will be reestablished.

EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, provides detailed guidance to campuses for creating, implementing, and maintaining a business continuity program that includes an ITDR plan. EO 1014 states that goals, which must be met by such a program, include, but are not limited to:

- Maintaining a program on each campus that ensures the continuity of essential functions or operations following a catastrophic event.
- Establishing recovery goals and objectives for the campus that reflect the needs of the campus and its business units.
- Identifying functions and assets that are essential to the operational continuity needed to support the campus’ mission.
- Recommending recovery strategies based on the circumstances of various events.
- Listing, prioritizing, and establishing recovery time objectives for essential functions, systems, and applications through business impact analyses and risk assessments.
- Establishing and testing alternate data processing capabilities, if deemed necessary.
- Protecting and safeguarding vital database systems and data assets.
- Reviewing, testing, modifying, and validating recovery plans in terms of campus and business unit expectations.

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, 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. While 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.
PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to ITDR planning and to determine the adequacy of controls that ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the audit objective, specific goals included determining whether:

- The administration of the ITDR program incorporates a defined mission, stated goals and objectives, and clear lines of organizational authority and responsibility, and is adequately funded.
- The ITDR plan is reviewed and modified on a regular basis, and modifications reflect the needs of the campus and the business units.
- Adequate system redundancy or alternate processes exist to ensure minimal interruption of critical business services.
- System backups and record retention are sufficient to meet the recovery objectives of the campus.
- Initiatives and investments are underway to improve ITDR planning and maximize ITDR resources; risks specific to the campus have been identified; and policies and procedures are current, comprehensive, and sufficient to support campus ITDR planning.
- 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 clearly identifies who has authority and responsibility for emergencies and incidents, and the emergency organization is sufficient to ensure that campus command/incident command techniques provide command and control when emergency incidents occur.
- ITDR resources are available; plans have been updated appropriately; and plans are integrated with the campus business continuity plan.
- Previous incidents were mitigated in a timely manner; lessons learned were evaluated; appropriate after-action reports were prepared; and sufficient plans for mitigation of any such incidents in the future are in place.
- Simulated tests of plan components are routinely scheduled, and after-action reports and modifications are generated.
- The potential outage times expected while executing the ITDR plan have been adequately communicated to and coordinated with the campus community, and emergency communications and operations are adequately coordinated and managed.
The campus business units have taken an active role in determining the prioritization of systems and their recovery time expectations.

Sufficient training has been provided to employees, disaster recovery staff, and building marshals who are expected to execute the ITDR plan, and the finance function has been integrated into the disaster recovery activities.

The ITDR plan is written so that a competent individual or group of individuals who are unfamiliar with the campus’ systems would be able to execute a portion or all of the recovery steps if needed.
The proposed scope of this audit was presented in Attachment A of Audit Agenda Item 2 during the January 25 and 26, 2011, meeting of the Committee on Audit. The attachment stated that the ITDR audit would include a review of Trustee policy, systemwide directives, campus policies and procedures, the essential functions or operations following a catastrophic event, business impact analysis and risk assessment, business continuity and disaster recovery plans, testing and exercising of plans, plan maintenance, communications, training, and necessary retention of key records.

The scope of this audit is focused on the campus’ ITDR planning specific to a disaster only affecting data processing services.

Our study and evaluation was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors and included the audit tests we considered necessary in determining that operational and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures in effect during fiscal year 2010/11. In instances wherein it was necessary to review annualized data, calendar years 2010 and 2011 were the periods reviewed.

Based upon this assessment of risks, we specifically included within the scope of our review the following:

- The ITDR planning management organization.
- The ITDR plan for all critical campus data processing activities.
- Disaster recovery plan guidelines, policies, procedures, and recordkeeping.
- The building marshal program, emergency action plans, and campus emergency hotline, as it relates to IT disasters.
- The EOC, emergency equipment, and related emergency supplies applicable to ITDR.
- Coordination with other agencies and vendors, including mutual aid and assistance.
- Funding and budgetary controls for disaster recovery planning activities.
- Communication of the disaster recovery plan.
- Training for emergency activities affecting data processing.
- Evacuation drills and emergency plan testing affecting campus data processing facilities.
- Backup and retention of system data.
OBSERVATIONS, RECOMMENDATIONS,
AND CAMPUS RESPONSES

ALTERNATE PROCESSING

The memorandum of understanding (MOU) between the campus and its designated long-term alternative processing (LTAP) site had not been formalized.

We noted that the campus had an email confirming that another campus would serve as its LTAP, but the email did not address the commitments and responsibilities of each party, such as effective dates, security measures specified, and levels of support.

State Administrative Manual (SAM) §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

SAM §20050 states, in part, that state entity heads are responsible for the establishment and maintenance of internal controls and administrative controls.

The vice president and chief information officer (CIO) stated that the MOU had not yet been formalized due to uncertainty surrounding the specifics of the alternate site configuration and a delay in identifying funding for disaster recovery equipment needed at the alternate site. He further stated that funding was identified for the 2011/12 fiscal year, and planning for the alternate site is in progress. In addition, he stated that the campus had developed a draft MOU based on similar disaster recovery MOUs from other California State University (CSU) institutions, and it will be formalized when specifics of the alternate disaster recovery site are finalized.

Failure to properly define alternative processing responsibilities can result in both financial and non-financial losses to the campus and the CSU and can result in unexpected delays in the recovery of data processing services.

Recommendation 1

We recommend that the campus formalize its MOU with its LTAP and define in detail the commitments and responsibilities of each party.

Campus Response

We concur. By January 31, 2012, a formal MOU will be executed with CSU Stanislaus that defines the alternate site responsibilities of each party.

BUSINESS CONTINUITY AND IMPACT ASSESSMENTS

The campus process for updating and reviewing business continuity plans (BCP) needed improvement.
We noted that:

- Several departmental BCPs had not been updated or reviewed on an annual basis.
- Some departmental BCPs, including the information technology (IT) plan, were not included in the campus BCP.

SAM §5355.1 states in part that the information technology disaster recovery (ITDR) plan shall be developed as part of a complete business continuity program that includes emergency response and business resumption plans. In addition, the agency should consider the results of its risk analysis and business impact analysis when developing its ITDR plan.

SAM §5305.1 states, in part, that the risk analysis be performed at least every two years and whenever there has been a significant change in the use of information technology.

Executive Order (EO) 1014, *Business Continuity*, dated October 2007, states, in part, that the business continuity plan should include, but not be limited to, a business impact analysis (BIA) and risk assessment. In addition, it states that the university should perform an administrative review of the BCP at least annually or more frequently as needed. Furthermore, it states that the campus shall have each critical business unit perform a BIA to determine the financial and non-financial losses associated with, among other items, a loss of data processing capabilities.

The associate vice president for risk management services stated that in 2007 the campus implemented a web-based BCP application that automated the process for monitoring plan development, review, and testing consistent with the requirements of EO 1014 and SAM. He further stated that since the implementation of the campus’ disaster recovery/BCP application in 2007, departments have consistently received annual automated email notifications reminding them of their responsibility to complete, review, and test their disaster recovery plans and BCPs. Finally, he stated that competing business priorities, other EO requirements, regulatory compliance demands, and the lack of people resources have thwarted departmental efforts to complete plans as required.

Failure to update and review BCPs in a timely manner, and failure to include all departmental BCPs in the campus BCP, increases the likelihood that the campus will not be adequately prepared or be able to effectively respond to an extended outage of data processing services.

**Recommendation 2**

We recommend that the campus develop and implement a process that ensures:

a. All departmental BCPs are updated and reviewed annually.

b. All departmental BCPs are included in the campus BCP.

**Campus Response**

We concur. By June 30, 2012, risk management will develop a BCP for the president’s approval, in compliance with EO 1014.
a. By June 30, 2012, risk management will implement a process related to the timely completion and annual review of departmental BCPs. The process will include:

- An annual continuity of operations/business continuity awareness and training campaign to inform organizations of the requirement to maintain a current continuity plan, train unit personnel regarding preparation of a continuity plan, and educate BCP coordinators on the use of CSU Sacramento’s BCP application.
- Regularly scheduled distribution of a report to all vice presidents and the president on completion and review status of departmental BCPs, so that administrators can initiate appropriate actions.

b. A department’s completed and approved BCP automatically becomes part of the campus BCP, as departmental plans are created, approved, and reside in CSU Sacramento’s existing online BCP system. By June 30, 2012, risk management will implement a business continuity process, which will record the requirement that departmental BCPs are included in the campus BCP.

END-USER COORDINATION AND RESTORATION PROCEDURES

Coordination between IT and business unit end-users needed improvement.

We found that:

- IT had not been informed of the various business units’ recovery expectations as documented in the BIA.
- The possibility of losing one week’s worth of data had not been communicated to the individual business units. For example, up to a week’s worth of data could be lost for critical systems such as Learning Management System and exchange email.

SAM §5355 states that agencies must have a plan that maintains viable strategies to ensure that critical information assets are available for continued business operations.

SAM §5355.1 states that disaster recovery plans and other IT procedures should be developed to ensure that critical services and applications are restored as quickly as possible and with minimal loss of data.

EO 1014, California State University Business Continuity Program, dated October 8, 2007, states that the campus shall have each critical business unit perform a BIA to determine the financial and non-financial losses associated with, among other items, a loss of data processing capabilities.

Integrated California State University Administrative Manual (ICSUAM) §8085.0, Business Continuity and Disaster Recovery, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster.
The vice president and chief information officer (CIO) stated that recovery expectations for critical information systems have been communicated to managers of the data contained in those systems, but not to all end users. He further stated that ITDR plan critical applications have been linked to both key end users and to business continuity planning through discussions between the vice president and CIO and the associate vice president for risk management, but the information was not disseminated to all end users. Finally, he stated that individual departments were not asked to consider the effects of losing one week’s worth of non-critical data because the IT department only considered the effects related to critical data and systems when preparing the ITDR plan.

Failure to understand the needs of the critical business units and to communicate the potential for lost data to end-users increases the likelihood that the campus will be unprepared to respond to a localized disaster, could significantly impact the campus’ ability to recover data processing services, and could result in permanent loss of transaction data.

**Recommendation 3**

We recommend that the campus:

a. Inform IT of the various business units’ recovery expectations as documented in the BIA.
b. Communicate the possibility of losing one week’s worth of data to the individual business units.

**Campus Response**

We concur.

a. Risk management has engaged the services of a web and database application developer to upgrade CSU Sacramento’s existing online BCP system. The upgraded online application will allow users to document organizational dependencies and recovery expectations and will associate those dependencies and expectations with the organization that provides the product or service, including information resources and technology (IRT). The provider will be automatically notified of those users dependent on its services, as well as the processes that are involved. Providers will then be able to use this information to appropriately guide their continuity planning. The vendor anticipates completion of the project by June 30, 2012.

b. By March 31, 2012, campus IRT will communicate the possibility of losing one week’s data from critical systems, due to a disaster occurring between weekly back-up time periods, to all applicable business units.

**DISASTER RECOVERY PLANNING**

**WRITTEN DISASTER RECOVERY PLAN**

The written ITDR plan needed improvement.
We noted that:

- The plan did not include all current systems and proper cross-references to other campus response plans that would be pertinent to a systematic recovery of data processing capabilities.

- The plan had not been formally approved.

- The plan did not include sufficient detail to allow a competent individual who is not directly familiar with each campus system to recover the application systems and hardware without undue delay, research, and/or guesswork.

SAM §5355.1 states, in part, that the ITDR plan shall be developed as part of a complete business continuity program, which includes emergency response and business resumption plans. In addition, the agency should consider the results of its risk analysis and business impact analysis when developing its ITDR plan. Furthermore, the ITDR plan process supports necessary preparation to identify and document procedures to recover critical operations in the event of an outage.

EO 1014, Business Continuity, dated October 2007, states in part that the BCP shall be approved/signed by the head of the business unit and the business continuity coordinator, or the business continuity planning committee.

The vice president and CIO stated that the campus used a formal approval process only for formal policy issues and that the campus was unaware of the requirement for a formally signed and dated ITDR plan. He further stated that the current ITDR plan is lacking in detail primarily because alternate site systems were recently purchased and are not yet set up at the alternate site.

Failure to maintain a properly approved and easily executable ITDR plan can result in unnecessary financial and non-financial losses in the event of a disaster and could significantly impact the campus’ ability to recover from a disaster affecting data processing services.

**Recommendation 4**

We recommend that the campus:

a. Update the ITDR plan to include current systems and proper cross-references to other campus response plans that would be pertinent to a systematic recovery of data processing capabilities.

b. Obtain formal approval of the ITDR plan.

c. Update the ITDR to include sufficient detail to allow an individual not directly familiar with each campus system to recover application systems and hardware without undue delay, research, and/or guesswork.
**Campus Response**

We concur.

a. By April 30, 2012, campus IRT will update the ITDR plan to include all applicable systems and will cross-reference to any applicable ITDR plans pertinent to the recovery of data processing capabilities.

b. By April 30, 2012, campus IRT will obtain formal approval of the ITDR plan by the vice president/CIO and president.

c. The update of the ITDR noted under Campus Response a. above will include sufficient detail to allow an individual familiar with applicable campus systems to recover hardware and software without undue delay.

**DISASTER RECOVERY PLAN TESTING**

The campus had not designed a comprehensive plan to test the recovery plan strategies.

SAM §5355.1 states that a disaster recovery plan should be designed such that the requirement for decision-making during and after an event is minimized and individuals are provided direction in as clear and concise a manner as possible. In addition, disaster recovery plans must be viable, fully documented, and tested.

EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, states that the campus must keep all business continuity-related plans current, must test all plans for viability, and must reference all materials necessary to recover from a disaster.

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states, in part, that campuses must ensure that information assets can continue to operate or be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster.

The vice president and CIO stated that the campus had conducted regular testing of disaster recovery procedures for critical systems, even though a comprehensive written testing plan had not been completed. He further stated that testing of alternate site systems had not occurred because those systems had not yet been installed off-site. In addition, he stated that comprehensive testing of campus data center systems critical to disaster recovery had occurred quarterly, including back-up generator, UPS, and generator fail-over, and that funding for replacement UPS batteries for disaster recovery was provided to information resources and technology in 2011/12.

The absence of a current, tested, and easily executable disaster recovery plan can result in unnecessary financial and non-financial losses in the event of a disaster and can create recovery delays that are outside of management expectations.
Recommendation 5

We recommend that the campus design a comprehensive plan to test the recovery plan strategies.

Campus Response

We concur. By April 30, 2012, campus IRT will update the ITDR, which will include a comprehensive plan to test applicable recovery plan strategies.
APPENDIX A:
PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexander Gonzalez</td>
<td>President</td>
</tr>
<tr>
<td>Mike Christensen</td>
<td>Associate Vice President of Risk Management Services</td>
</tr>
<tr>
<td>Larry Gilbert</td>
<td>Vice President and Chief Information Officer, Information Resources and Technology</td>
</tr>
<tr>
<td>Ted Koubiar</td>
<td>Director of Operations and System Services</td>
</tr>
<tr>
<td>Ming-Tung “Mike” Lee</td>
<td>Interim Vice President and Chief Financial Officer, Administration and Business Affairs</td>
</tr>
<tr>
<td>Kathi McCoy</td>
<td>Director of Auditing Services</td>
</tr>
<tr>
<td>Lucinda Parker</td>
<td>Project and Policy Manager</td>
</tr>
<tr>
<td>Greg Porter</td>
<td>Director of Networking and Telecommunications</td>
</tr>
<tr>
<td>Kirt Stout</td>
<td>Director of Risk Management and Business Continuity Planning</td>
</tr>
</tbody>
</table>
December 15, 2011

Larry Mandel
University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802-4210

SUBJECT: Campus Response to Recommendations
         IT Disaster Recovery Audit, Report #11-31

Dear Mr. Mandel:

Please find attached California State University, Sacramento’s response to the recommendations of the audit. The campus is committed to addressing and resolving the issues identified in the audit report.

If you have any questions or require additional information, please contact Kathi McCoy, Director of Auditing Services, at (916) 278-7439.

Sincerely,

Ming-Tung "Mike" Lee, Ph.D.
Vice President & Chief Financial Officer (Interim)

MTL:kd

Attachment

cc: Alexander Gonzalez, President
Larry Gilbert, Vice President and Chief Information Officer
Mike Christensen, Associate Vice President for Risk Management
Kathi McCoy, Director of Auditing Services
IT DISASTER RECOVERY
CALIFORNIA STATE UNIVERSITY,
SACRAMENTO
Audit Report 11-31

ALTERNATE PROCESSING

Recommendation 1

We recommend that the campus formalize its MOU with its LTAP and define in detail the commitments and responsibilities of each party.

Campus Response

We concur. By January 31, 2012, a formal MOU will be executed with CSU Stanislaus that defines the alternate site responsibilities of each party.

BUSINESS CONTINUITY AND IMPACT ASSESSMENTS

Recommendation 2

We recommend that the campus develop and implement a process that ensures:

a. All departmental BCPs are updated and reviewed annually.
b. All departmental BCPs are included in the campus BCP.

Campus Response

We concur. By June 30, 2012, Risk Management will develop a Business Continuity Policy for president's approval, in compliance with EO 1014.

a. By June 30, 2012, Risk Management will implement a process related to the timely completion and annual review of departmental BCPs. The process will include:

- Annual Continuity of Operations/Business Continuity awareness and training campaign
  - Inform organizations of the requirement to maintain a current continuity plan
  - Train unit personnel regarding preparation of a continuity plan
  - Educate BCP coordinators on the use of Sacramento State's BCP application

- Regularly scheduled distribution of a report to all vice presidents and the president on completion and review status of departmental BCPs, so that administrators can initiate appropriate actions
b. A department’s completed and approved business continuity plan automatically becomes part of the campus BCP, as departmental plans are created, approved, and reside in Sacramento State’s existing, online BCP system. By June 30, 2012, Risk Management will implement a business continuity process, which will record the requirement that departmental BCPs are included in the campus BCP.

END-USER COORDINATION AND RESTORATION PROCEDURES

Recommendation 3

We recommend that the campus:

a. Inform IT of the various business units’ recovery expectations as documented in the BIA.
b. Communicate the possibility of losing one week’s worth of data to the individual business units.

Campus Response

We concur.

a. Risk Management has engaged the services of a web and database application developer to upgrade Sacramento State’s existing, online BCP system. The upgraded online application will allow users to document organizational dependencies and recovery expectations, and will associate those dependencies and expectations with the organization that provides the product or service, including IRT. The provider will be automatically notified of those users dependent on their services, as well as the processes that are involved. Providers will then be able to use this information to appropriately guide their continuity planning. The vendor anticipates completion of the project by June 30, 2012.

b. By March 31, 2012, campus IRT will communicate the possibility of losing one week’s data from critical systems, due to a disaster occurring between weekly back-up time periods, to all applicable business units.

DISASTER RECOVERY PLANNING

WRITTEN DISASTER RECOVERY PLAN

Recommendation 4

We recommend that the campus:

a. Update the ITDR plan to include current systems and proper cross-references to other campus response plans that would be pertinent to a systematic recovery of data processing capabilities.
b. Obtain formal approval of the ITDR plan.
c. Update the ITDR to include sufficient detail to allow an individual not directly familiar with each campus system to recover application systems and hardware without undue delay, research, and/or guesswork.

_Campus Response_

We concur.

a. By April 30, 2012, campus IRT will update the ITDR plan to include all applicable systems and will cross-reference to any applicable IT disaster response plans pertinent to recovery of data processing capabilities.

b. By April 30, 2012, campus IRT will obtain formal approval of the ITDR plan by the Vice President & CIO and President.

c. The update of the ITDR noted under a. above will include sufficient detail to allow an individual familiar with applicable campus systems to recover hardware and software without undue delay.

**DISASTER RECOVERY PLAN TESTING**

_Recommendation 5_

We recommend that the campus design a comprehensive plan to test the recovery plan strategies.

_Campus Response_

We concur. By April 30, 2012, campus IRT will update the ITDR, which will include a comprehensive plan to test applicable recovery plan strategies.
January 3, 2012

MEMORANDUM

TO: Mr. Larry Mandel
   University Auditor

FROM: Charles B. Reed
       Chancellor

SUBJECT: Draft Final Report 11-31 on IT Disaster Recovery,
         California State University, Sacramento

In response to your memorandum of January 3, 2012, I accept the response as
submitted with the draft final report on IT Disaster Recovery, California State
University, Sacramento.

CBR/amd