IT DISASTER RECOVERY

CALIFORNIA STATE UNIVERSITY,
BAKERSFIELD

Audit Report 10-36
December 17, 2010

Members, Committee on Audit

Henry Mendoza, Chair
Raymond W. Holdsworth, Vice Chair
Nicole M. Anderson  Margaret Fortune
George G. Gowgani  Melinda Guzman
William Hauck

Staff

University Auditor:  Larry Mandel
Senior Director:  Michelle Schlack
Audit Manager:  Greg Dove

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
CONTENTS

APPENDICES

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

ABBREVIATIONS

CSU California State University
EO Executive Order
EOC Emergency Operations Center(s)
FISMA Financial Integrity and State Manager’s Accountability
ICSUAM Integrated California State University Administrative Manual
ITDR Information Technology Disaster Recovery
SAM State Administrative Manual
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2009, the Board of Trustees, at its January 2010 meeting, directed that Information Technology Disaster Recovery (ITDR) 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 (FISMA) and Auxiliary Organization audits.

We visited the California State University, Bakersfield campus from July 19, 2010, through July 22, 2010, 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 control over the following areas: business impact assessment, end-user coordination and restoration procedures, and disaster recovery planning. 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 July 22, 2010, 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 of 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.

BUSINESS IMPACT ASSESSMENT [7]

The campus had completed a business impact assessment, but it had not determined the specific recovery timelines, nor had it determined whether the ITDR plan satisfied the business requirements.

END-USER COORDINATION AND RESTORATION PROCEDURES [8]

IT recovery expectations had not been clearly communicated to the individual business units.

DISASTER RECOVERY PLANNING [9]

The written plan for the recovery of IT services needed improvement. In addition, the campus had not designed a comprehensive plan to test the IT services recovery plan strategy.
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 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 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.
INTRODUCTION

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.
INTRODUCTION

- 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 26 and 27, 2010, 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 2009/10. In instances wherein it was necessary to review annualized data, calendar years 2009 and 2010 were the periods reviewed.

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

BUSINESS IMPACT ASSESSMENT

Business continuity planning needed improvement.

We noted that the campus had completed a business impact assessment, but it had not determined the specific recovery timelines, nor had it determined whether the information technology disaster recovery (ITDR) plan satisfied business requirements.

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 §5355.2 states that each agency must maintain a disaster recovery plan that identifies the systems critical to the agency’s operations, the information assets required to operate the systems, and a tested process by which the systems will be restored.

Executive Order (EO) 1014, California State University Business Continuity Plan, dated October 8, 2007, states that the campus must develop plans to protect all critical data assets to ensure minimum data loss and continued business functionality in the event of a disaster.

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 assistant vice president of IT stated that the ITDR plans were based on the IT department’s estimation of a reasonable recovery time that would not generate extensive costs, but that defined business recovery time frames would help to refine the recovery alternatives and validate the existing plan.

Failure to determine the business impact of a loss of data processing services prevents the campus from providing realistic expectations for the recovery planning for such services.

Recommendation 1

We recommend that the campus determine the specific business recovery timelines and evaluate whether the ITDR plan satisfies business requirements.

Campus Response

We concur. The campus will evaluate its business continuity plan and tie in specific ITDR requirements. In addition, the campus will adjust the ITDR plan to address critical IT services that may be required in the event of a disaster. Estimated completion date is December 31, 2011.
END-USER COORDINATION AND RESTORATION PROCEDURES

IT recovery expectations had not been clearly communicated to the individual business units.

Specifically, we noted that the campus had not coordinated with the individual business units to convey that:

- Data processing outages may last for an extended period of time, and manual desk procedures would need to be followed until the systems could be restored.
- Because the nightly backup tapes were stored in the data center, some data could be completely lost, and manual recovery procedures should include a step to verify the state of the recovered data and determine which data must be re-created from alternative sources.

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 business impact assessment to determine the financial and non-financial losses associated with, among other items, a loss of data processing capabilities.

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 critical business services are restored with minimal interruption in the event of a disaster.

The assistant vice president of IT stated that the campus had recently conducted a business impact survey and that data recovery expectations would be included in the ongoing planning process. The vice president of business and administrative services stated that manual desk procedures existed for most departments, but the procedures did not include steps for reconciling the status of recovered data or for re-creating data that may have been lost during the system failure.

Failure to understand the needs of the critical business units and not communicating potential outage impacts to end users 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:

a. Communicate the possible length of data processing outage and lost data to the individual business units.

b. Update the end-user manual processing desk procedure to include provisions for reconciling the status of the recovered system and re-creating lost data.

Campus Response

We concur.

a. The university will establish a periodic communication to the university community outlining the potential of data loss and outage of IT services. Expected completion date is December 31, 2011.

b. The campus will create guidelines for university departments for their development of business processes to deal with an IT disaster. Expected completion date is December 31, 2011.

DISASTER RECOVERY PLANNING

WRITTEN DISASTER RECOVERY PLAN

The written plan for the recovery of IT services needed improvement.

We noted that existing disaster recovery plan documentation:

- Did not cross-reference other plans that contain steps that are essential to a recovery process, such as the campus’ emergency procedures, escalation and notification procedures, and use of the emergency command center and public communications.

- Did not include specific plans for recovery of an event affecting the telecommunications facility, which would disable all access to the core campus systems located in Salt Lake City.

- Included plans for a duplexed virtual environment that did not exist.

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. Also, 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 assistant vice president of IT stated his belief that the disaster recovery plan made it clear that data processing services would follow the emergency preparedness plan in the event of a disaster. He further stated that failure to plan for an outage affecting the telecommunications facility was due to oversight and that the referenced duplexed environment was planned but had not yet been approved or implemented.

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 3**

We recommend that the campus amend the plan for the recovery of IT services to include specific references to the campus’ emergency procedures, escalation and notification procedures, use of the emergency command center and public communications, and a recovery plan in the event of an outage at the telecommunications facility. The plan should not include references to future processes that do not exist.

**Campus Response**

We concur. The university will integrate its ITDR plan with the campus’ emergency procedures, escalation and notification procedures, and the campus business continuity plan, when completed. Expected completion date is December 31, 2011.

**DISASTER RECOVERY PLAN TESTING**

The campus had not designed a comprehensive plan to test the IT services recovery plan strategy.

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 critical business services are restored with minimal interruption in the event of a disaster.
The assistant vice president of IT stated that some aspects of the recovery strategy had been informally tested through periodic interruptions of service and through load testing, but that formal detailed tests of the overall recovery plan had not been routinely performed.

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 4**

We recommend that the campus design a comprehensive plan to test the IT services recovery plan strategy.

**Campus Response**

We concur. The university will develop a plan to test the IT services recovery strategies and technical infrastructure. Expected completion date is December 31, 2011.
## APPENDIX A:
### PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horace Mitchell</td>
<td>President</td>
</tr>
<tr>
<td>Mike Fleming</td>
<td>Network Analyst</td>
</tr>
<tr>
<td>Michael Neal</td>
<td>Vice President, Business and Administrative Services</td>
</tr>
<tr>
<td>Clark Sanford</td>
<td>Assistant Vice President, Information Technology</td>
</tr>
<tr>
<td>Doug Wade</td>
<td>Assistant Vice President, Fiscal Services</td>
</tr>
<tr>
<td>Dave Watts</td>
<td>Director, Telecommunications</td>
</tr>
</tbody>
</table>
February 8, 2011

Mr. Larry Mandel
University Auditor
Office of the Chancellor
California State University
401 Golden Shore, 4th Floor
Long Beach, CA 90802-4210

Re: University's Responses to Recommendations contained in IT Disaster Recovery Audit Report #10-36

Dear Mr. Mandel:

Attached are the University's responses to the recommendations contained in Audit Report #10-36.

If you have any further questions please contact my office at 661-654-2287

Sincerely,

[Signature]

Michael A. Neal
Vice President for Business and Administrative Services

Enclosure

c: Horace Mitchell, CSUB President
    Douglas Wade, Assistant Vice President, Fiscal Services
IT DISASTER RECOVERY
CALIFORNIA STATE UNIVERSITY,
BAKERSFIELD
Audit Report 10-36

BUSINESS IMPACT ASSESSMENT

Recommendation 1

We recommend that the campus determine the specific business recovery timelines and evaluate whether the ITDR plan satisfies business requirements.

Campus Response

We concur. The campus will evaluate its business continuity plan and tie in specific IT disaster recovery requirements. In addition, the campus will adjust the ITDR plan to address critical IT services that may be required in the event of a disaster. Estimated completion date is December 31, 2011.

END-USER COORDINATION AND RESTORATION PROCEDURES

Recommendation 2

We recommend that the campus:

a. Communicate the possible length of data processing outage and lost data to the individual business units.

b. Update the end-user manual processing desk procedure to include provisions for reconciling the status of the recovered system and re-creating lost data.

Campus Response

We concur.

a. The University will establish a periodic communication to the University Community, outlining the potential of data loss and outage of IT Services. Expected completion date is December 31, 2011.

b. The campus will create guidelines for University departments for their development of business processes to deal with an IT disaster. Expected completion date is December 31, 2011.
DISASTER RECOVERY PLANNING

WRITTEN DISASTER RECOVERY PLAN

Recommendation 3

We recommend that the campus amend the plan for the recovery of IT services to include specific references to the campus’ emergency procedures, escalation and notification procedures, use of the emergency command center and public communications, and a recovery plan in the event of an outage at the telecommunications facility. The plan should not include references to future processes that do not exist.

Campus Response

We concur. The University will integrate its IT Disaster Recovery plan with the campus’ emergency procedures, escalation and notification procedures, and the campus Business Continuity Plan, when completed. Expected completion date is December 31, 2011.

DISASTER RECOVERY PLAN TESTING

Recommendation 4

We recommend that the campus design a comprehensive plan to test the IT services recovery plan strategy.

Campus Response

We concur. The University will develop a plan to test the IT services recovery strategies and technical infrastructure. Expected completion date is December 31, 2011.
MEMORANDUM

TO: Mr. Larry Mandel  
University Auditor

FROM: Charles B. Reed  
Chancellor

SUBJECT: Draft Final Report 10-36 on IT Disaster Recovery, California State University, Bakersfield

February 23, 2011

In response to your memorandum of February 23, 2011, I accept the response as submitted with the draft final report on IT Disaster Recovery, California State University, Bakersfield.

CBR/amd