IT DISASTER RECOVERY

CALIFORNIA STATE UNIVERSITY,
NORTHRIDGE

Audit Report 10-37
February 3, 2011

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

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

Introduction ................................................................................................................................. 2
  Background ............................................................................................................................... 2
  Purpose ................................................................................................................................... 4
  Scope and Methodology .......................................................................................................... 6

OBSERVATIONS, RECOMMENDATIONS, 
AND CAMPUS RESPONSES

Departmental Disaster Recovery Planning .............................................................................. 7
APPENDICES

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

ABBREVIATIONS

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, Northridge campus from October 25, 2010, through November 3, 2010, and audited the procedures in effect at that time.

Our study and evaluation did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on ITDR controls. However, we did identify other reportable weaknesses that are described in the executive summary and body of this report. In our opinion, the operational and administrative controls for ITDR activities in effect as of November 3, 2010, taken as a whole, were 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.

DEPARTMENTAL DISASTER RECOVERY PLANNING [7]

The housing department’s ITDR plan did not include a sufficient level of detail to ensure that its in-house-developed resident database system could be recovered in a timely manner, and the library and student affairs departments had not documented the impact of potentially losing one week’s worth of transaction data.
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 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 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.

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.
DEPARTMENTAL DISASTER RECOVERY PLANNING

Information technology disaster recovery (ITDR) planning in various campus areas needed improvement.

Specifically, we found that:

- The housing department's ITDR plan did not include a sufficient level of detail to ensure that its in-house-developed resident database system could be recovered in a timely manner.

- The library and student affairs departments had not documented the impact of losing one week's worth of transaction data in their ITDR plans.

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 §5355.1 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.

Executive Order 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.

Integrated California State University Administrative Manual §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 chief information officer stated that all systems determined to be mission-critical to the ongoing operation of the campus had been identified and detailed corresponding plans had been developed for these systems. She also stated that the departmental systems identified in the audit were not identified as mission-critical to the ongoing operation of the campus and thus were not included in the California State University, Northridge ITDR planning under her purview. The housing coordinator for information systems stated that the specifics of backup and recovery for its resident database had not been documented due to oversight. The student affairs technology director stated that central IT performs daily backup and has procedures in place for weekly off-site storage. He further stated that the data in question was not mission-critical to student affairs and that it was due to oversight that the impact of losing one week's data was not documented. The library systems administrator stated that the loss of a week's worth of library records would not prevent ongoing operations, but that consideration should be given to minimizing the loss of any data records.
Failure to document the recovery strategy and timelines and failure to consider the potential for lost data could result in an unexpected disruption of campus services and could result in permanent loss of transaction data.

**Recommendation 1**

We recommend that the campus:

a. Ensure that the housing department’s ITDR plan includes sufficient detail to ensure that its in-house-developed resident database system could be recovered in a time frame that satisfies management expectations.

b. Ensure that the library and student affairs departments document the impact of losing one week’s worth of transaction data in their ITDR plans.

**Campus Response**

We concur.

a. The housing department’s ITDR plan has been revised to include sufficient detail to ensure that its resident database system can be recovered.

b. The library and student affairs departments have documented the impact of losing one week’s worth of transaction data in their ITDR plans.
### APPENDIX A:
PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jolene Koester</td>
<td>President</td>
</tr>
<tr>
<td>Hilary Baker</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Keith Blaine</td>
<td>Housing Coordinator for Information Systems</td>
</tr>
<tr>
<td>Don Foster</td>
<td>Operations Lead</td>
</tr>
<tr>
<td>Kevin Krzewinski</td>
<td>Director Database Systems and Identity Management</td>
</tr>
<tr>
<td>Will Moran</td>
<td>Network Engineering Lead</td>
</tr>
<tr>
<td>Tom McCarron</td>
<td>Vice President of Administration and Finance and Chief Financial Officer</td>
</tr>
<tr>
<td>Chris Olsen</td>
<td>Senior Director, Information Security Officer</td>
</tr>
<tr>
<td>Ben Quillian</td>
<td>Associate Vice President of Administration and User Support Services (at time of review)</td>
</tr>
<tr>
<td>Paul Schantz</td>
<td>Director, Student Affairs Technology</td>
</tr>
<tr>
<td>Eric Willis</td>
<td>Library Systems Administrator</td>
</tr>
</tbody>
</table>
February 16, 2011

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

Subject: Campus Response to Recommendations of Audit Report Number 10-37,

*IT Disaster Recovery* at California State University, Northridge

Dear Larry:

Enclosed please find the California State University, Northridge (CSUN) response to the recommendations of the audit, as requested in your email of February 8, 2011.

We have read the report including the observations and recommendations, and agree with them. Corrective action to implement all of the recommendations has been taken. By separate correspondence, the applicable documents evidencing completion of our implementation process and corrective action for each recommendation will be provided.

Should there be questions regarding the contents of the response, they may be addressed to Howard Lutwak, CSUN Internal Audit Director at (818) 677-2333.

We appreciate the recommendations to improve CSUN’s systems of internal control.

Sincerely,

[Signature]

Tom McCarron
Vice President Administration and Finance and CFO

TM: mh

Enclosures

cc: Jolene Koester, President
Howard Lutwak, Director, Internal Audit
DEPARTMENTAL DISASTER RECOVERY PLANNING

Recommendation 1

We recommend that the campus:

a. Ensure that the housing department’s ITDR plan includes sufficient detail to ensure that its in-house-developed resident database system could be recovered in a time frame that satisfies management expectations.

b. Ensure that the library and student affairs departments document the impact of losing one week’s worth of transaction data in their ITDR plans.

Campus Response

We concur.

a. The housing department’s ITDR plan has been revised to include sufficient detail to ensure that its resident database system can be recovered.

b. The library and student affairs departments have documented the impact of losing one week’s worth of transaction data in their ITDR plans.
March 11, 2011

MEMORANDUM

TO: Mr. Larry Mandel
    University Auditor

FROM: Charles B. Reed
      Chancellor

SUBJECT: Draft Final Report 10-37 on *IT Disaster Recovery*,
         California State University, Northridge

In response to your memorandum of March 11, 2011, I accept the response as submitted with the draft final report on *IT Disaster Recovery*, California State University, Northridge.

CBR/amd