IT DISASTER RECOVERY

CALIFORNIA STATE UNIVERSITY,
DOMINGUEZ HILLS

Audit Report 11-33
August 18, 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
Senior Director: Michael Caldera
Audit Manager: Greg Dove
Senior Auditor: Gordon Eng

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

End-User Coordination and Restoration Procedures .................................................................................... 7

Disaster Recovery Planning .......................................................................................................................... 8
  Equipment Replacement Coverage........................................................................................................... 8
  Written Disaster Recovery Plan ................................................................................................................ 9
  Test Plans ................................................................................................................................................ 10
APPENDICES

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

ABBREVIATIONS

CIO Chief Information Officer
EO Executive Order
EOC Emergency Operations Center(s)
FISMA Financial Integrity and State Manager’s Accountability Act
ICSUAM Integrated California State University Administrative Manual
IT Information Technology
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 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 (FISMA) and Auxiliary Organization audits.

We visited the California State University, Dominguez Hills campus from June 6, 2011, through June 17, 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: 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 June 17, 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.

END-USER COORDINATION AND RESTORATION PROCEDURES [7]

Coordination between information technology (IT) and the business units needed improvement. Specifically, a campuswide business impact analysis had not been performed.

DISASTER RECOVERY PLANNING [8]

The campus had not provided its equipment replacement vendor with an updated configuration listing, as required by the vendor’s contract, and did not have a process to ensure that the vendor received such listings. Also, the written IT disaster recovery plan needed improvement. For example, the plan did not cross-reference other plans that contain steps essential to a recovery process, such as the campus’ emergency procedures, escalation and notification procedures, use of the emergency command center, and public communications. Finally, the campus had not designed a comprehensive plan to test the IT services recovery 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 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.
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.
SCOPE AND METHODOLOGY

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

END-USER COORDINATION AND RESTORATION PROCEDURES

Coordination between information technology (IT) and the business units needed improvement.

We found that a campuswide business impact analysis had not been performed, and IT was unaware of the recovery expectations of the various business units.

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 (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.

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 for administration and finance stated that during the process of creating the disaster recovery plan in 2003, it was assumed that the campus had conducted a business impact analysis, but there was no written documentation for this action.

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

Recommendation 1

We recommend that the campus conduct a campuswide business impact analysis that includes the recovery expectations of the various business units.

Campus Response

We concur. The campus will conduct a campuswide business impact analysis that includes the recovery expectations of the various business units.

Expected completion date: December 2011
DISASTER RECOVERY PLANNING

EQUIPMENT REPLACEMENT COVERAGE

The campus had not provided its equipment replacement vendor with an updated configuration listing, as required by the vendor’s contract, and did not have a process to ensure that the vendor received such listings.

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.

The associate vice president and chief information officer (CIO) stated that the vendor had visited the campus in October when the contract was written to verify equipment types and amounts but did not have an updated report of server and network configuration due to oversight, and the oversight was corrected immediately.

Failure to provide current equipment information to vendors as required by the contract increases the likelihood that the vendors will not deliver equipment configurations needed to operate campus systems and could increase the anticipated time frame for recovery.

Recommendation 2

We recommend that the campus:

a. Provide the equipment replacement vendor with an updated server and network configuration listing.

b. Implement a process to ensure that the vendor receives updated configuration listings in the future.

Campus Response

We concur.

a. The campus has provided the equipment replacement vendor with an updated server and network configuration listing.

b. The campus has implemented a process to ensure that the vendor receives updated configuration listings in the future.

Corrective action on this issue is complete.
WRITTEN DISASTER RECOVERY PLAN

The written IT disaster recovery (ITDR) plan needed improvement.

We noted that the plan:

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

- Did not address recovery strategies in the event of an outage affecting the telecommunications facility, which would disable all access to the critical campus systems located in Salt Lake City.

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 associate vice president and CIO stated that the campus had considered a total telecommunications repair job order as its recovery strategy; however, going forward, it will repair the potential point of failure in the telecommunications and networking. He also stated that the campus is in the process of coordinating and cross-referencing the ITDR plan with campus emergency procedures and the use of the emergency command center and its communications capability.

The absence of a current 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 written ITDR plan to include:

a. Cross-references to other plans that contain steps essential to a recovery process, such as the campus’ emergency procedures, escalation and notification procedures, use of the emergency command center, and public communications.

b. Recovery strategies in the event of an outage affecting the telecommunications facility.
Campus Response

We concur.

a. The campus will amend the written ITDR plan to include cross references to other plans such as the campus emergency procedures, escalation and notification procedures and use of the EOC.

b. The campus will develop a recovery strategy in the event of an outage affecting the telecommunications facility.

Expected completion date: January 2012

TEST PLANS

The campus had not designed a comprehensive plan to test the IT services recovery 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 minimal interruption of critical business services occurs in the event of a disaster.

The associate vice president and CIO stated that although the campus routinely tests the restoration of all tape/disk backups, a comprehensive plan to test telecommunications and network failures was not established. He also stated that going forward, a test plan would be developed and performed on a routine basis.

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 strategy.
Campus Response

We concur. The campus will develop a comprehensive plan to test the IT services recovery strategy.

Expected completion date: December 2011
### APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mildred Garcia</td>
<td>President</td>
</tr>
<tr>
<td>Ron Bergmann</td>
<td>Associate Vice President and Chief Information Officer, Information Technology</td>
</tr>
<tr>
<td>James Bersig</td>
<td>Director, Administrative Information and Common Management Systems</td>
</tr>
<tr>
<td>Danny Lujan</td>
<td>Director, Networking, Telecommunications, and Help Desk Services</td>
</tr>
<tr>
<td>Mary Ann Rodriquez</td>
<td>Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Jonathan Scheffler</td>
<td>Associate Director, Physical Plant</td>
</tr>
<tr>
<td>Gary Singer</td>
<td>Emergency Management and Preparedness Coordinator, Risk Management/Environmental Health and Occupational Safety</td>
</tr>
<tr>
<td>Karen Wall</td>
<td>Associate Vice President, Administration and Finance</td>
</tr>
</tbody>
</table>
September 7, 2011

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

Dear Mr. Mandel:

Enclosed, please find California State University, Dominguez Hills’ responses to the IT Disaster Recovery Audit Report 11-33, dated August 18, 2011. The campus is committed to addressing and resolving the issues identified in the audit report.

If you have any questions or would like additional information, please contact me.

Sincerely,

Mary Ann Rodriguez
Vice President, Administration and Finance

Enclosure (1)

c: Mildred Garcia, President
    Karen Wall, Associate Vice President, Administration and Finance
END-USER COORDINATION AND RESTORATION PROCEDURES

Recommendation 1

We recommend that the campus conduct a campuswide business impact analysis that includes the recovery expectations of the various business units.

Campus Response

We concur. The campus will conduct a campuswide business impact analysis that includes the recovery expectations of the various business units.

Expected completion date: December 2011

DISASTER RECOVERY PLANNING

EQUIPMENT REPLACEMENT COVERAGE

Recommendation 2

We recommend that the campus:

a. Provide the equipment replacement vendor with an updated server and network configuration listing.

b. Implement a process to ensure that the vendor receives updated configuration listings in the future.

Campus Response

We concur.

a. The campus has provided the equipment replacement vendor with an updated server and network configuration listing.

b. The campus has implemented a process to ensure that the vendor receives updated configuration listings in the future.

Corrective action on this issue is complete.
WRITTEN DISASTER RECOVERY PLAN

Recommendation 3

We recommend that the campus amend the written ITDR plan to include:

a. Cross-references to other plans that contain steps essential to a recovery process, such as the campus’ emergency procedures, escalation and notification procedures, use of the emergency command center, and public communications.

b. Recovery strategies in the event of an outage affecting the telecommunications facility.

Campus Response

We concur.

a. The campus will amend the written ITDR plan to include cross references to other plans such as the campus emergency procedures, escalation and notification procedures and use of the emergency command center.

b. The campus will develop a recovery strategy in the event of an outage affecting the telecommunications facility.

Expected completion date: January 2012

TEST PLANS

Recommendation 4

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

Campus Response

We concur. The campus will develop a comprehensive plan to test the IT services recovery strategy.

Expected completion date: December 2011
September 20, 2011

MEMORANDUM

TO: Mr. Larry Mandel
University Auditor

FROM: Charles B. Reed
Chancellor

SUBJECT: Draft Final Report 11-33 on IT Disaster Recovery,
California State University, Dominguez Hills

In response to your memorandum of September 20, 2011, I accept the response as submitted with the draft final report on IT Disaster Recovery, California State University, Dominguez Hills.

CBR/amd