IT DISASTER RECOVERY

CALIFORNIA STATE UNIVERSITY,
MONTEREY BAY

Audit Report 10-35
October 6, 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
Senior Auditor:  Eric Wilson

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**

Backup Procedures ........................................................................................................................................ 8

End-User Coordination and Restoration Procedures .................................................................................. 9

Disaster Recovery Planning .......................................................................................................................... 10

Restart Recovery ....................................................................................................................................... 11
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
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 Act (FISMA) and Auxiliary Organization audits.

We visited the California State University, Monterey Bay campus from June 28, 2010, through July 2, 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 July 2, 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 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.

BACKUP PROCEDURES [8]

The campus had not taken appropriate steps to ensure that critical information systems data would be available in the event of a localized disaster. Further, the campus had not determined what amount of data loss would be acceptable by the business units and had not created a schedule to move backup media off-site accordingly.

END-USER COORDINATION AND RESTORATION PROCEDURES [9]

Information Technology was unaware of the data processing capabilities expected by end users, and end users were unaware of the length of time potential data processing outages could last. Also, the campus had not formally designated which individuals or entities owned the campus’ various critical data assets.

DISASTER RECOVERY PLANNING [10]

The campus’ ITDR plan needed further development. Specifically, it did not include a contingency plan for the operation of the payroll department and had not been tested in a disaster recovery simulation.
RESTART RECOVERY [11]

The campus had not established which business systems were critical to its operation and had not developed the disaster recovery plan’s restart and recovery activities accordingly.
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 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.
OBSERVATIONS, RECOMMENDATIONS,
AND CAMPUS RESPONSES

BACKUP PROCEDURES

The campus had not adequately ensured that information systems data would be available in the event of a localized disaster affecting the data center.

We found that a process had not been developed for the transfer of backup media off-site based on the determination of the appropriate amount of data loss that would be acceptable to 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 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 chief information officer (CIO) stated that not having the backup system physically separated from the main data center was an oversight.

Failure to determine what amount of data loss is acceptable to end users and not creating a backup plan that reflects such a loss can result in significant disruptions to campus operations and exposes the campus to legal and financial damages.

Recommendation 1

We recommend that the campus adequately ensure that information systems data would be available in the event of a localized disaster affecting the data center by developing a process for the transfer of backup media from the main data center to an off-site storage location on a daily basis.

Campus Response

We concur. We are developing plans to modify backup processes and procedures to minimize potential data loss. We expect to complete this work by January 11, 2011.
END-USER COORDINATION AND RESTORATION PROCEDURES

The campus’ coordination between IT and business unit end users required improvement.

We found that:

- Because a campus-wide end-user impact analysis had not been performed, IT was unaware of recovery expectations of the various business units.

- The length of time required for the restoration of data processing capabilities after a disaster had not been communicated to business units.

- The data owners of critical data assets had not been identified.

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 minimal interruption of critical business services occurs in the event of a disaster.

The CIO stated that due to scheduling constraints, the campus had not completed the end-user business impact analysis. He also stated that the lack of formal communication with end users and the absence of assigned data ownership was the result of administrative oversight.

Failure to understand the needs of the critical business units and to communicate potential outage times to end users increases the likelihood that the campus will be unprepared to respond to a localized disaster and could significantly impact the campus’ ability to recover data processing services. Failure to formally establish which individuals or entities own critical data assets may result in a lack of managerial accountability and can lead to confusion in the event of a loss of data assets.

Recommendation 2

We recommend that the campus:

a. Perform a campus-wide business impact analysis to determine which business units are critical and what the acceptable time frames for data processing outage are for each.
b. Inform the various business units of the length of time they could be without data processing services following a disaster affecting the data center.

c. Identify the data owners for critical data assets.

**Campus Response**

We concur. We are currently performing a business impact analysis and identifying data owners. This data will be used to construct a communications plan to inform system users and data owners of potential service interruptions in the event of system failures. We expect to complete this work by March 8, 2011.

**DISASTER RECOVERY PLANNING**

The campus’ ITDR plan required further development.

We found that the current ITDR plan:

- Did not include a contingency plan for the operation of the payroll department, which relies on certified terminals to process business-critical data.
- Had not been tested in a simulated disaster recovery.

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 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 CIO stated that the lack of contingency planning regarding the payroll department was the result of the challenges associated with establishing a second physical connection to the State Controller’s Office. He also stated that there was an informal contingency plan for the payroll department that involved using another campus to process the critical data. In addition, the CIO stated that the lack of disaster recovery simulations was the result of not viewing standard maintenance activities as opportunities to simulate disaster recovery activities.
The absence of a contingency plan for departments that require unique hardware and/or applications to process critical data may result in a loss of data and a failure to maintain operational continuity. The lack of a current, tested, and easily executable disaster recovery plan could result in unnecessary financial and non-financial losses in the event of a disaster and could significantly impact the campus’ ability to recovery from a disaster affecting data processing services.

**Recommendation 3**

We recommend that the campus:

a. Develop a contingency plan for the payroll department that will allow for the processing of critical data in the event of a local disaster.

b. Test the ITDR plan in a simulated disaster recovery and implement a process to modify it based on the test results.

**Campus Response**

We concur. We are developing a contingency and test plan for payroll data processing. We expect to complete this work by January 11, 2011.

**RESTART RECOVERY**

The campus had not designated which systems are considered critical to its business operations nor structured the recovery activities in a manner that reflects the prioritization of the critical systems.

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 CIO stated that the lack of understanding regarding the critical business functions and associated IT systems was the result of not integrating the various informal campus ITDR plans into a central plan that had received management review and approval.

Failure to designate which systems are critical to business operations and failure to develop a recovery plan that prioritizes the systems could lead to unnecessary data processing downtime and a loss of business continuity.
Recommendation 4

We recommend that the campus:

a. Formally designate which systems are critical to the campus’ business operations.

b. Structure the disaster recovery plan’s recovery activities in a manner that reflects the prioritization of the critical systems.

Campus Response

We concur. We are currently performing a business impact analysis. This data will be used to identify critical systems and system recovery priorities in the ITDR plan. We expect to complete this work by March 8, 2011.
## APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dianne Harrison</td>
<td>President</td>
</tr>
<tr>
<td>Jerry Figuerres</td>
<td>Risk Manager</td>
</tr>
<tr>
<td>John Fitzgibbon</td>
<td>Associate Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Asuman Johnson</td>
<td>Associate Director, Information Systems</td>
</tr>
<tr>
<td>Chip Lenno</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Steven Mann</td>
<td>Senior Operations Analyst</td>
</tr>
<tr>
<td>Mary Mauro</td>
<td>Manager, Campus Data Warehouse</td>
</tr>
<tr>
<td>Kevin Saunders</td>
<td>Interim Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Eric Simoni</td>
<td>Associate Director, Information Systems</td>
</tr>
<tr>
<td>Henry Simpson</td>
<td>Director, Technology Support Services</td>
</tr>
<tr>
<td>Rick Skibiniski</td>
<td>Network Engineering Analyst</td>
</tr>
<tr>
<td>Chris Taylor</td>
<td>Executive Director, Collaborative Technology Initiatives</td>
</tr>
</tbody>
</table>
November 4, 2010

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

Subject: IT Disaster Recovery Audit #10-35

Dear Larry:

Attached is the hard copy of CSU Monterey Bay’s response to the recommendations regarding the subject audit. Electronic copy has been transmitted to you.

Please contact AVP John Fitzgibbon if you have any questions or comments.

Sincerely,

Kevin Saunders  
Interim Vice President

Attachment

Cc: Senior Director Schlack  
Provost Cruz-Urbie  
CIO Lenno  
Assoc VP Fitzgibbon
IT DISASTER RECOVERY
CALIFORNIA STATE UNIVERSITY,
MONTEREY BAY
Audit Report 10-35

BACKUP PROCEDURES

Recommendation 1

We recommend that the campus adequately ensure that information systems data would be available in the event of a localized disaster affecting the data center by developing a process for the transfer of backup media from the main data center to an off-site storage location on a daily basis.

Campus Response

The campus concurs and is developing plans to modify its backup processes and procedures to minimize potential data loss. The campus expects to complete this work by January 11, 2011.

END-USER COORDINATION AND RESTORATION PROCEDURES

Recommendation 2

We recommend that the campus:

a. Perform a campus-wide business impact analysis to determine which business units are critical and what the acceptable timeframes for data processing outage are for each.

b. Inform the various business units of the length of time they could be without data processing services following a disaster affecting the data center.

c. Identify the data owners for critical data assets.

Campus Response

The campus concurs and is currently performing a business impact analysis and identifying data owners. This data will be used to construct a communications plan to inform system users and data owners of potential service interruptions in the event of system failures. The campus expects to complete this work by March 8, 2011.
DISASTER RECOVERY PLANNING

Recommendation 3

We recommend that the campus:

a. Develop a contingency plan for the payroll department that will allow for the processing of critical data in the event of a local disaster.

b. Test the ITDR plan in a simulated disaster recovery and implement a process to modify it based on the test results.

Campus Response

The campus concurs and is developing a contingency and test plan for payroll data processing. The campus expects to complete this work by January 11, 2011.

RESTART RECOVERY

Recommendation 4

We recommend that the campus:

a. Formally designate which systems are critical to the campus’ business operations.

b. Structure the disaster recovery plan’s recovery activities in a manner that reflects the prioritization of the critical systems.

Campus Response

The campus concurs and is currently performing a business impact analysis. This data will be used to identify critical systems and system recovery priorities in the ITDR Plan. The campus expects to complete this work by March 8, 2011.
November 24, 2010

MEMORANDUM

TO: Mr. Larry Mandel
   University Auditor

FROM: Charles B. Reed
      Chancellor

SUBJECT: Draft Final Report 10-35 on *IT Disaster Recovery*,
         California State University, Monterey Bay

In response to your memorandum of November 24, 2010, I accept the response
as submitted with the draft final report on *IT Disaster Recovery*, California
State University, Monterey Bay.

CBR/amd