IT DISASTER RECOVERY
SYSTEMWIDE

Audit Report 11-35
March 28, 2012

Members, Committee on Audit

Henry Mendoza, Chair
William Hauck   Steven M. Glazer
Glen O. Toney

Staff

University Auditor: Larry Mandel
Senior Directors: Michelle Schlack and Michael Caldera
IT Audit Manager: Greg Dove
Senior Auditors: Gordon Eng, Eric Wilson, and Salesian Yuen
Internal Auditor: Sal Rodriguez

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Background</td>
<td>3</td>
</tr>
<tr>
<td>Purpose</td>
<td>5</td>
</tr>
<tr>
<td>Scope and Methodology</td>
<td>7</td>
</tr>
<tr>
<td><strong>OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES</strong></td>
<td></td>
</tr>
<tr>
<td>Offsite Alternate Processing Facility</td>
<td>8</td>
</tr>
<tr>
<td>Business Continuity Planning for CMS</td>
<td>9</td>
</tr>
<tr>
<td>IT Disaster Recovery Plans</td>
<td>10</td>
</tr>
</tbody>
</table>
APPENDICES

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

ABBREVIATIONS

CMS Common Management Systems
CO Chancellor’s Office
CSU California State University
DRP Disaster Recovery Plan
EO Executive Order
EOC Emergency Operations Center
FISMA Financial Integrity and State Manager’s Accountability
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 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 12 campuses from April 19, 2010, through June 30, 2011, and audited the procedures in effect at that time. Campus-specific findings and recommendations have been discussed and reported individually.

Our study and evaluation revealed certain conditions that, in our opinion, could result in significant risk exposures if not corrected. Specifically, the campuses did not maintain adequate internal control over the following areas: business impact assessment, alternate processing, and disaster recovery planning. These conditions 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 30, 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.

OFFSITE ALTERNATE PROCESSING FACILITY [8]

Most campuses had not planned for remote restoration of processing capabilities after a disaster. Specifically, campus personnel had plans to relocate to another data processing facility on campus, but the plans did not include relocation to a remote location in the event of a campuswide disaster; some campuses had a memorandum of understanding with another California State University (CSU) campus to provide remote alternative processing capabilities, but this approach was not consistent among the campuses audited.

BUSINESS CONTINUITY PLANNING FOR CMS [9]

The campuses were not made aware of the potential impact to their operations in the event of a disaster affecting the Common Management System (CMS) processing center in Salt Lake City. Specifically, the campuses were unaware of the disaster recovery contractual commitment between the CSU and Unisys, the facility operator, and did not understand where the systems would be relocated after a disaster, how long they might need to operate manually, and how much data could be lost and would need to be...
re-created. In addition, the campus business continuity plans did not include procedures for re-creating lost CMS transactions or for determining the state of the CMS upon its restoration.

**IT DISASTER RECOVERY PLANS [10]**

Most campuses had significant deficiencies in their written information technology (IT) disaster recovery plans (DRP). Specifically, each campus had completed a written IT DRP, but many of those plans did not address critical IT functions or lacked consistent coordination with other campus business continuity plans.
INTRODUCTION

BACKGROUND

Information Technology Disaster Recovery (ITDR) planning is a specific subset of an entity’s business continuity planning process that addresses how the IT resources required to operate critical business functions will be restored in a timely and effective manner following a disaster. ITDR planning requires the interaction of individuals at every level of an organization and a recognition by the organization that, in today’s computer-driven work environment, the loss of data processing capabilities can lead to significant financial loss and non-financial exposures if an organization has not planned properly for such an occurrence.

The ITDR planning process requires the evaluation and consideration of several factors, including:

- Who will coordinate the recovery activities, and which supporting groups will report to that coordinator.

- How business units will be impacted if data processing capabilities are lost.

- Which IT systems are critical to support those business units.

- How systems will be restored in the event of a disaster, whether alternate processing facilities will be necessary, whether backup hardware should be stockpiled, and whether insurance coverage will be needed to cover the costs of recovery activities.

- The kind of training individuals involved with the recovery activities will need to ensure they will be prepared to respond to a disaster in a concise and coordinated manner.

- What incidents have occurred in the past that tested the recovery capabilities of the IT systems, how plans have been modified as a result of the incidents, and what simulated testing is required to refine the effectiveness of the plan.

Because organizational and operational design variances exist between the 23 campuses and the Office of the Chancellor, each campus process must consider many unique factors. Campuses have been directed to prepare ITDR plans for disasters via multiple directives, including, but not limited to, State Administrative Manual (SAM) §5355-5355.2, Executive Order (EO) 1014, and the Integrated California State University Administrative Manual (ICSUAM) §8085.0.

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

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

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

ICSUAM §8085.0, *Business Continuity and Disaster Recovery*, dated April 19, 2010, represents the most recent and specific guidance to campuses in regard to ITDR planning. Simply stated, the policy directs campuses to ensure that information assets can continue to operate or, in a reasonable time frame, be supplanted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster or other emergency event. While the policy itself does not provide detailed operational requirements, it can be surmised that the campuses must consider a multitude of factors such as restart times, backup and recovery procedures, system security (environmental, physical, and logical), and system interdependence and redundancy to ensure a satisfactory level of continued operational capacity.
PURPOSE

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

Within the audit objective, specific goals included determining whether:

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

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

The ITDR plan is written so that a competent individual or group of individuals who are unfamiliar with the campus’ systems would be able to execute a portion or all of the recovery steps if needed.
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 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 MANAGEMENT RESPONSES

OFFSITE ALTERNATE PROCESSING FACILITY

Most campuses had not planned for remote restoration of processing capabilities after a campuswide disaster.

We found that all of the campuses we visited had developed a plan to relocate data processing capabilities to another facility on campus in the event of a disaster affecting the processing facility, but those plans did not include a provision to relocate to a remote location in the event of a disaster affecting the entire campus. Some campuses had memorandums of understanding with another California State University (CSU) campus to provide a remote alternative processing facility, but this approach was not consistent.

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 that are 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 supplan ted by backup systems so that minimal interruption of critical business services occurs in the event of a disaster.

The campus chief information officers stated that their plans for restoration of processing capabilities did not address relocation to a remote location after a campuswide disaster because if such a disaster were to occur, the business operations would also be disrupted and the expectation of data processing recovery would not be as immediate; therefore, they would have more time to establish remote processing capabilities.

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

Recommendation 1

We recommend that the chancellor’s office (CO):

a. Evaluate the possibility of establishing remote alternative processing centers at certain campuses.

b. Communicate the recovery strategy to the campuses.
Management Response

We concur. The CO will evaluate the possibility of establishing a shared data center environment for use by the campuses as a disaster recovery resource. This will be accomplished by December 2012.

BUSINESS CONTINUITY PLANNING FOR CMS

The campuses were not made aware of the potential impact to their operations in the event of a disaster affecting the Common Management System (CMS) processing center in Salt Lake City.

We found that the campuses were unaware of the disaster recovery contractual commitment between the CSU and Unisys, the facility operator. Specifically, the campuses did not understand where the systems would be relocated after a disaster, how long they might need to operate manually, and how much data could be lost and would need to be re-created. In addition, the campus business continuity plans did not include procedures for re-creating lost CMS transactions or for determining the state of the CMS upon its restoration.

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 that are 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.

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.

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 campus business continuity coordinators stated that they had not been informed of the CMS recovery strategy and were unaware of any impact to the campus communities of a loss of data processing services following a disaster affecting the CMS processing center in Salt Lake City.

Failure to adequately determine the business impact of a loss of data processing services prevents the campuses from determining how long business operations could continue before they would suffer severe degradation of business services or excessive monetary loss, and prevents the campus from providing realistic expectations for the recovery of data processing services.

Recommendation 2

We recommend that the CO inform the campuses of the CMS recovery strategy and ensure that the campuses align their business continuity plans and manual operating procedures with this strategy.
Management Response

We concur. Campuses will be informed that they align their business continuity plans and manual operating procedures with the CMS recovery strategy. The campuses also will be provided the link/location of the CMS recovery strategy. This will be completed by November 2012.

IT DISASTER RECOVERY PLANS

Most campuses had significant deficiencies in their written information technology (IT) disaster recovery plans (DRP).

We found that each campus had completed a written IT DRP, but many of those plans did not address critical IT functions or lacked consistent coordination with other campus business continuity plans. Specifically, we found that campus IT DRPs:

- Often omitted recovery of network services that were housed outside of the data center.
- Were not consistently coordinated and aligned with the business continuity plans. Further, campus expectations for the recovery of data processing services, as determined in the business impact assessment, were not always communicated to the IT departments.
- Did not include adequate coordination of recovery strategies among decentralized campus IT departments.
- Did not consistently cross-reference other plans that contained 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 provide a step-by-step set of instructions detailing what, when, where, and how action should be taken immediately preceding, during, and following an emergency event, or who should be performing each action.
- Did not contain sufficient detail to allow a competent individual who is not directly familiar with the campus’ IT operations to restore the systems and hardware without undue delay, research, and/or guesswork.
- Did not include adequate plans for testing the recovery of data processing services.

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 campus business continuity coordinators stated numerous reasons for the omissions, including oversight of operations being housed outside of the data center, ongoing development of the campus business continuity planning process, and the lack of consistent governance and oversight regarding overall responsibility for business continuity planning.

The absence of a current, tested, and easily executable IT DRP 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 CO:

a. Remind the campuses that they are required to complete a comprehensive business continuity plan that includes recovery of data processing services.

b. Ensure that the annual review of campus business continuity plans certifies that recovery of data processing services is included in the overall continuity plan.

**Management Response**

We concur. A reminder will be sent to the campuses that the annual review of campus business continuity plans certifies that recovery of data processing services is included in their overall continuity plan. This will be completed by November 2012.
# APPENDIX A:
## PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office of the Chancellor</strong></td>
<td></td>
</tr>
<tr>
<td>Benjamin F. Quillian</td>
<td>Executive Vice Chancellor and Chief Financial Officer</td>
</tr>
<tr>
<td>Bruce Briggs</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Lori Erdman</td>
<td>Chief of Staff, Business and Finance</td>
</tr>
<tr>
<td>Zachery Gifford</td>
<td>Associate Director, California State University Claims Office</td>
</tr>
<tr>
<td>Charlene Minnick</td>
<td>Assistant Vice Chancellor, Systemwide Risk Management and Public Safety</td>
</tr>
<tr>
<td>Cheryl Washington</td>
<td>Chief Information Officer (At time of review)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>California State University, Bakersfield</th>
<th></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>

<table>
<thead>
<tr>
<th>California State University, Channel Islands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Richard R. Rush</td>
<td>President</td>
</tr>
<tr>
<td>Herbert Aquino</td>
<td>Manager of Academic and Information Technology Infrastructure</td>
</tr>
<tr>
<td>Michael Berman</td>
<td>Interim Vice President for Finance and Administration/Chief Information Officer (At</td>
</tr>
<tr>
<td></td>
<td>time of review)</td>
</tr>
<tr>
<td>Joanne Coville</td>
<td>Vice President for Finance and Administration (At time of review)</td>
</tr>
<tr>
<td>Marc DuBranasky</td>
<td>Senior Systems Administrator</td>
</tr>
<tr>
<td>Judy Frazier</td>
<td>Administrative Analyst</td>
</tr>
<tr>
<td>Ernesto Gutierrez</td>
<td>Senior Network Analyst</td>
</tr>
<tr>
<td>Michael Long</td>
<td>Senior Telecommunications Analyst</td>
</tr>
<tr>
<td>Ysabel Trinidad</td>
<td>Vice President, Finance and Administration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>California State University, Dominguez Hills</th>
<th></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 Rodriques</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>
APPENDIX A: PERSONNEL CONTACTED

California State University, East Bay
Leroy M. Morishita President
Mohammad H. Qayoumi President (At time of review)
Rich Avila Director, Server and Network Operations
Shawn Bibb Vice President, Administration and Finance (At time of review)
Lee Breitzman Lead Operations Specialist, Server Operations
John Charles Chief Information Officer
Matt Collins Director, Application Systems
Chris Da Silva Network Analyst
Thomas Dixon Network Security Analyst
Brad Wells Interim Vice President, Administration and Chief Financial Officer

California State University, Los Angeles
James M. Rosser President
Lisa Chavez Vice President, Administration and Chief Financial Officer
Tanya Ho University Auditor
Robert Hoffman Assistant Director, Network Operations, Servers and Technology Operations
Greg King Director of Public Safety and University Police
Karen Melick Director, Administrative Technology
Sheryl Okuno Director, IT Security and Compliance
Peter Quan Vice President and Chief Technology Officer, Information Technology Services
Chris Rapp Director, IT Infrastructure Services
Sal Rodriguez Senior Auditor

California Maritime Academy
William B. Eisenhardt President
Walter Abaca Network Analyst
Jannette Corpus Director of Information Technology
Raj Duraisamy Computer Programmer
Stephen Frazier Chief Information Officer
Kurt Lohide Vice President, Administration and Finance
Raul Lucky Network Operation Center Manager
Mark Nickerson Vice President, Administration and Finance (At time of review)
Roseann Richard Chief of Police
Mark Stackpole Library Technician
Ken Toet Controller
Ryan Wold Webmaster

California State University, Monterey Bay
Dianne F. Harrison President
Jerry Figuerres Risk Manager
John Fitzgibbon Associate Vice President, Administration and Finance
Asuman Johnson Associate Director, Information Systems
Chip Lenno Chief Information Officer
Steven Mann Senior Operations Analyst
Mary Mauro Manager, Campus Data Warehouse
APPENDIX A: PERSONNEL CONTACTED

California State University, Monterey Bay (cont.)
Kevin Saunders  Vice President, Administration and Finance
Eric Simoni  Associate Director, Information Systems
Henry Simpson  Director, Technology Support Services
Rick Skibiniski  Network Engineering Analyst
Chris Taylor  Executive Director, Collaborative Technology Initiatives

California State University, Northridge
Harold Hellenbrand  Interim President
Jolene Koester  President (At time of review)
Hilary Baker  Chief Information Officer
Keith Blaine  Housing Coordinator for Information Systems
Don Foster  Operations Lead
Kevin Krzewinski  Director Database Systems and Identity Management
Howard Lutwak  Director of Internal Audit
Will Moran  Network Engineering Lead
Tom McCarron  Vice President of Administration and Finance and Chief Financial Officer
Chris Olsen  Senior Director, Information Security Officer
Ben Quillian  Associate Vice President of Administration and User Support Services (At time of review)
Paul Schantz  Director, Student Affairs Technology
Eric Willis  Library Systems Administrator

California State Polytechnic University, Pomona
J. Michael Orti  President
Albert Arboleda  Information Security Officer
Edwin Barnes  Vice President/Chief Financial Officer, Administrative Affairs
Stephanie Doda  Chief Information Officer
Lisa Dye  Business Continuity Coordinator
Timothy He  Information Technology Consultant, Library Systems
Joe Matsumoto  Director, Instructional and Information Technology Systems
Debbi McFall  Emergency Services Coordinator
Kevin Morningstar  Executive Director, Student Affairs Technology Service
Susan Reese  Manager, Instructional and Information Technology Systems Projects and Services
Glendy Yeh  Executive Director, Administrative Affairs Information Systems

California State University, Sacramento
Alexander Gonzalez  President
Mike Christensen  Associate Vice President of Risk Management Services
Larry Gilbert  Vice President and Chief Information Officer, Information Resources and Technology
Ted Koubiar  Director of Operations and System Services
Ming-Tung “Mike” Lee  Interim Vice President and Chief Financial Officer, Administration and Business Affairs
Kathi McCoy  Director of Auditing Services
Lucinda Parker  Project and Policy Manager
APPENDIX A: PERSONNEL CONTACTED

California State University, Sacramento (cont.)
Greg Porter  Director of Networking and Telecommunications
Kirt Stout  Director of Risk Management and Business Continuity Planning

California State University, San Bernardino
Albert K. Karnig  President
Laura Carrizales  Information Security Analyst
Lorraine Frost  Interim Vice President, Information Resources and Technology
Robert Gardner  Vice President of Administration and Finance
Melissa Spagnuolo  Confidential Administrative Support
Javier Torner  Interim Associate Vice President and Information Security Officer

California State University, San Francisco
Robert A. Corrigan  President
Maggie Beers  Director, Academic Technology
Heather Boshears Robbins  Internal Auditor
Taver Chong  Associate Internal Auditor
Michael Cramer  Information Technology Consultant
Tuan Do  Assistant Director, Systems Support Group
Nancy Hayes  Interim Vice President of Administration and Finance
Phoebe Kwan  Interim Chief Information Officer and Associate Vice President
Michael Lam  Information Technology Consultant
Leroy M. Morishita  Executive Vice President and Chief Financial Officer
(At time of review)
Teresa Ono  Advancement Services Manager
Alastair Smith  Director Student Health Services
Jack Tse  Senior Director, Network and Operations and Chief Operations Officer
Corazon Wong  Director, Student Financial Operations and Fiscal Affairs
    Business Systems
MEMORANDUM

DATE: May 10, 2012

TO: Larry Mandel
   University Auditor

FROM: Benjamin F. Quillian
   Executive Vice Chancellor and
   Chief Financial Officer

SUBJECT: Management Response to Recommendations in Audit Report #11-35,
   IT Disaster Recovery, Systemwide

In response to the “Preliminary Draft” report dated February 9, 2012, we are providing
the enclosed management responses.

Should you have any questions, please feel free to contact Bruce Briggs or myself.

BFQ:ije

Attachment

c: Bruce Briggs, Assistant Vice Chancellor/CIO, Information Technology
   Charlene Minnick, Assistant Vice Chancellor, Risk Management & Public Safety
   William Perry, Chief Information Security Officer
IT DISASTER RECOVERY
SYSTEMWIDE
Audit Report 11-35

OFFSITE ALTERNATE PROCESSING FACILITY

Recommendation 1

We recommend that the chancellor’s office (CO):

a. Evaluate the possibility of establishing remote alternative processing centers at certain campuses.
b. Communicate the recovery strategy to the campuses.

Management Response

We concur. The CO will evaluate the possibility of establishing a shared data center environment for use by the campuses as a disaster recovery resource. This will be accomplished by December 2012.

BUSINESS CONTINUITY PLANNING FOR CMS

Recommendation 2

We recommend that the CO inform the campuses of the CMS recovery strategy and ensure that the campuses align their business continuity plans and manual operating procedures with this strategy.

Management Response

We concur. Campuses will be informed that they align their business continuity plans and manual operating procedures with the CMS recovery strategy. The campuses also will be provided the link/location of the CMS recovery strategy. This will be completed by November 2012.

IT DISASTER RECOVERY PLANS

Recommendation 3

We recommend that the CO:

a. Remind the campuses that they are required to complete a comprehensive business continuity plan that includes recovery of data processing services.
b. Ensure that the annual review of campus business continuity plans certifies that recovery of data processing services is included in the overall continuity plan.
Management Response

We concur. A reminder will be sent to the campuses that the annual review of campus business continuity plans certifies that recovery of data processing services is included in their overall continuity plan. This will be completed by November 2012.
May 25, 2012

MEMORANDUM

TO: Mr. Larry Mandel  
    University Auditor

FROM: Charles B. Reed  
    Chancellor

SUBJECT: Draft Final Report 11-35 on *IT Disaster Recovery, Systemwide*

In response to your memorandum of May 25, 2012, I accept the response as submitted with the draft final report on *IT Disaster Recovery, Systemwide.*

CBR/amd