IT DISASTER RECOVERY
SAN FRANCISCO STATE UNIVERSITY

Audit Report 11-32
August 25, 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: Salesian Yuen

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

Disaster Recovery Planning ......................................................................................................................... 8

Alternative Processing ............................................................................................................................... 9
  Campus Memorandum of Understanding ............................................................................................... 9
  Departmental Computing Alternative Processing ............................................................................... 9

Backup Procedures ................................................................................................................................... 10

Disaster Recovery Plan Coordination ....................................................................................................... 11

Disaster Recovery Tests ............................................................................................................................ 12
APPENDICES

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

ABBREVIATIONS

AT  Academic Technology
CIO  Chief Information Officer
CSUF California State University, Fullerton
EO  Executive Order
EOC Emergency Operations Center(s)
ICSUAM Integrated California State University Administrative Manual
IT  Information Technology
ITDR Information Technology Disaster Recovery
IT DRP Information Technology Disaster Recovery Plan
MOU Memorandum of Understanding
SAM State Administrative Manual
SFSU San Francisco State University
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 San Francisco State University campus from May 23, 2011, through June 10, 2011, 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 June 10, 2011, 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.

DISASTER RECOVERY PLANNING [8]

The campus information technology disaster recovery plan (IT DRP) did not include specific recovery timelines that aligned with the recovery time requirements defined in the business impact analysis.

ALTERNATIVE PROCESSING [9]

The campus had not established a memorandum of understanding with its alternative processing facility at California State University, Fullerton. In addition, administration of alternative processing for the academic technology (AT) department needed improvement. Specifically, AT had not established an alternate processing facility to be used in the event of a disaster, and it did not have a plan for obtaining replacement equipment in a timely manner during a disaster.

BACKUP PROCEDURES [10]

Backup tapes were not always stored at an off-site location.
EXECUTIVE SUMMARY

DISASTER RECOVERY PLAN COORDINATION [11]

Campus IT departments had not adequately coordinated their IT DRPs.

DISASTER RECOVERY TESTS [12]

The campus had not developed a comprehensive plan to test the disaster recovery plans for the IT and AT divisions.
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.
INTRODUCTION

PURPOSE

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

Within the audit objective, specific goals included determining whether:

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

DISASTER RECOVERY PLANNING

The campus information technology disaster recovery plan (IT DRP) did not include specific recovery timelines that aligned with the recovery time requirements defined in the business impact analysis.

Executive Order (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 IT DRP. It further states that goals, which must be met by such a program, include, but are not limited to, the listing, prioritizing, and establishing of recovery time objectives for essential functions, systems, and applications through business impact analyses and risk assessments.

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 information technology (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 interim chief information officer (CIO) stated that specific recovery timelines were prepared but were not included in the IT DRP due to management oversight.

Failure to create a complete IT DRP could lead to misunderstandings and confusion of management expectations for recovery of operations.

Recommendation 1

We recommend that the campus revise the IT DRP to include specific timelines that align with the recovery time requirements defined in the business impact analysis.

Campus Response

We are using SF State Ready, a product based on the open-source tool Kuali Ready, to maintain individual unit business continuity and disaster recovery plans in our decentralized environment. The Division of IT will hardcode into the SF State Ready system more specific and granular recovery timelines. We will include four or five categories using the examples provided by the California State University Office of the University Auditor as guidance.

Estimated completion: October 1, 2011
ALTERNATIVE PROCESSING

CAMPUS MEMORANDUM OF UNDERSTANDING

The campus had not established a memorandum of understanding (MOU) with its alternative processing facility at California State University, Fullerton (CSUF).

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 interim CIO stated that the reciprocal agreement between the IT divisions at San Francisco State University (SFSU) and CSUF had not been signed because the agreement terms were not yet finalized and approved by all relevant parties.

The absence of fully executed agreements subjects the campus to potential liability and increases the risk of misunderstandings and confusion of management expectations for recovery of operations.

Recommendation 2

We recommend that the campus establish an MOU with its alternate processing facility at CSUF.

Campus Response

The MOU was finalized with the relevant signatures of SFSU and CSUF parties during audit fieldwork.

DEPARTMENTAL COMPUTING ALTERNATIVE PROCESSING

Administration of alternative processing for the academic technology (AT) department needed improvement.

Specifically, we noted that AT:

- Had not established an alternate processing facility to be used in the event of a disaster.
- Did not have a plan for obtaining replacement equipment in a timely manner during a disaster.

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 director of AT stated that she had begun negotiating with the campus IT department for use of their alternative processing facilities but had not yet formalized the arrangement due to oversight.

Failure to adequately document the recovery strategy, including the alternative processing facilities and equipment replacement plans, subjects the campus to potential liability and increases the risk of misunderstandings and confusion of management expectations for recovery of operations.

**Recommendation 3**

We recommend that the campus ensure that:

a. AT establishes an alternative processing facility to be used in the event of a disaster and updates its IT DRP accordingly.

b. AT develops a plan for obtaining replacement equipment in a timely manner during a disaster.

**Campus Response**

The campus will take the following actions:

a. The director of AT will establish an agreement with an alternate processing facility to be used in the event of a disaster and will update its DRP accordingly. This will include working with the Division of IT to consider adding AT to existing university agreements.

b. AT will provide a list of replacement equipment needed to the interim CIO for inclusion in the existing contract that covers replacement equipment to be provided in a disaster.

Estimated completion: October 1, 2011

**BACKUP PROCEDURES**

Backup tapes were not always stored at an off-site location.

We found that AT stored backup tapes of its data in a fire-resistant safe across campus.

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 IT DRP, 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.
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.

Integrated California State University Administrative Manual (ICSUAM) §8085.0, Business Continuity and Disaster Recovery, dated April 19, 2010, states that campuses must 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. This includes considering 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.

The director of AT stated that backup tapes were not stored at an off-site location due to oversight.

Failure to store backup tapes at an off-site location can lead to data being inaccessible during recovery of operations.

**Recommendation 4**

We recommend that the campus instruct AT to store its backup tapes at an off-site location.

**Campus Response**

AT will send encrypted backup tapes to an off-site location. AT will join the existing contract the Division of IT currently has with Iron Mountain that covers off-site storage of backup tapes.

Estimated completion: November 1, 2011

**DISASTER RECOVERY PLAN COORDINATION**

Campus IT departments had not adequately coordinated their IT DRPs.

We noted that:

- Recovery expectations were different among IT departments.

- The division of IT had not communicated its disaster recovery plans and impact to other campus IT departments.

- The division of IT had not synchronized its IT DRP with those of other campus IT departments.

EO 1014, *California State University Business Continuity Program*, dated October 8, 2007, lists goals, which must be met by such a program, and includes establishing and testing alternate data processing capabilities, if deemed necessary.
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 information technology (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 interim CIO stated that the campus had recently implemented efforts to enhance coordination among the decentralized IT units and was continuously striving to improve coordination across units.

Failure to coordinate disaster recovery planning across all IT units could lead to misunderstandings and confusion of management expectations for recovery of operations.

**Recommendation 5**

We recommend that the campus adequately coordinate all campus IT DRPs.

**Campus Response**

Units house their individual business continuity and disaster recovery plans on SF State Ready. We are implementing more specific and granular recovery timelines as discussed above in Campus Response 1. The Campus Technology Committee (CTC), a governance group with cross-campus representation, will create a working group to address coordination and synchronization of campus DRPs.

Estimated completion: April 30, 2012

**DISASTER RECOVERY TESTS**

The campus had not developed a comprehensive plan to test the disaster recovery plans for the IT and AT divisions.

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 interim CIO stated that the campus is in the process of developing a test plan.

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 6**

We recommend that the campus develop comprehensive plans to test the disaster recovery plans for the IT and AT divisions.

**Campus Response**

The CTC working group referred to in Campus Response 5 will be tasked with developing and implementing a comprehensive plan for periodic testing of IT and AT division DRPs.

Estimated completion: April 30, 2012
## APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert A. Corrigan</td>
<td>President</td>
</tr>
<tr>
<td>Maggie Beers</td>
<td>Director, Academic Technology</td>
</tr>
<tr>
<td>Heather Boshears Robbins</td>
<td>Internal Auditor</td>
</tr>
<tr>
<td>Taver Chong</td>
<td>Associate Internal Auditor</td>
</tr>
<tr>
<td>Michael Cramer</td>
<td>Information Technology Consultant</td>
</tr>
<tr>
<td>Tuan Do</td>
<td>Assistant Director, Systems Support Group</td>
</tr>
<tr>
<td>Nancy Hayes</td>
<td>Interim Vice President of Administration and Finance</td>
</tr>
<tr>
<td>Phoebe Kwan</td>
<td>Interim Chief Information Officer and Associate Vice President</td>
</tr>
<tr>
<td>Michael Lam</td>
<td>Information Technology Consultant</td>
</tr>
<tr>
<td>Leroy M. Morishita</td>
<td>Executive Vice President and Chief Financial Officer</td>
</tr>
<tr>
<td></td>
<td>(At time of review)</td>
</tr>
<tr>
<td>Teresa Ono</td>
<td>Advancement Services Manager</td>
</tr>
<tr>
<td>Alastair Smith</td>
<td>Director Student Health Services</td>
</tr>
<tr>
<td>Jack Tse</td>
<td>Senior Director, Network and Operations and Chief Operations Officer</td>
</tr>
<tr>
<td>Corazon Wong</td>
<td>Director, Student Financial Operations and Fiscal Affairs</td>
</tr>
<tr>
<td></td>
<td>Business Systems</td>
</tr>
</tbody>
</table>
October 3, 2011

Mr. Larry Mandel
University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802-4275

Dear Mr. Mandel:

We have reviewed the Office of the University Auditor Report #11-32, IT Disaster Recovery at San Francisco State University. Our responses to the recommendations are being provided to your office electronically. Documentation demonstrating implementation of recommendations as they are completed will be sent to you separately.

Questions regarding the responses may be directed to Nancy K. Hayes, Interim Vice President for Administration & Finance at 415/338-2521 or to Heather Boshears Robbins, Internal Auditor at 415/405-4343.

Sincerely,

Robert A. Corrigan
President

HBR/id

Attachment

cc: Nancy K. Hayes, Interim Vice President, Administration & Finance
    Heather Boshears Robbins, Internal Auditor
DISASTER RECOVERY PLANNING

Recommendation 1

We recommend that the campus revise the IT DRP to include specific timelines that align with the recovery time requirements defined in the business impact analysis.

Campus Response

We are using SF State Ready, a product based on the open source tool Kuali Ready, to maintain individual unit business continuity and disaster recovery plans in our decentralized environment. The Division of IT will hardcode into the SF State Ready system more specific and granular recovery timelines. We will include four or five categories using the examples provided by the CSU Office of the University Auditor as guidance.

Estimated completion: October 1, 2011

ALTERNATIVE PROCESSING

CAMPUS MEMORANDUM OF UNDERSTANDING

Recommendation 2

We recommend that the campus establish an MOU with its alternate processing facility at CSUF.

Campus Response

The MOU was finalized with the relevant signatures of SFSU and CSUF parties during audit fieldwork.

DEPARTMENTAL COMPUTING ALTERNATIVE PROCESSING

Recommendation 3

We recommend that the campus ensure that:

a. AT establishes an alternative processing facility to be used in the event of a disaster and updates its IT DRP accordingly.
b. AT develops a plan for obtaining replacement equipment in a timely manner during a disaster.

**Campus Response**

The campus will take the following actions:

a. The director of AT will establish an agreement with an alternate processing facility to be used in the event of a disaster and will update its DRP accordingly. This will include working with the Division of IT to consider adding AT to existing university agreements.

b. AT will provide a list of replacement equipment needed to the Interim CIO for inclusion in the existing contract that covers replacement equipment to be provided in a disaster.

Estimated completion: October 1, 2011

**BACKUP PROCEDURES**

**Recommendation 4**

We recommend that the campus instruct AT to store its backup tapes at an off-site location.

**Campus Response**

AT will send encrypted backup tapes to an offsite location. AT will join the existing contract the Division of IT currently has with Iron Mountain that covers offsite storage of backup tapes.

Estimated completion: November 1, 2011

**DISASTER RECOVERY PLAN COORDINATION**

**Recommendation 5**

We recommend that the campus adequately coordinate all campus IT DRPs.

**Campus Response**

Units house their individual business continuity and disaster recovery plans on SF State Ready. We are implementing more specific and granular recovery timelines as discussed above in Campus Response #1. The Campus Technology Committee (CTC), a governance group with cross-campus representation, will create a working group to address coordination and synchronization of campus DRPs.

Estimated completion: April 30, 2012
DISASTER RECOVERY TESTS

Recommendation 6

We recommend that the campus develop comprehensive plans to test the disaster recovery plans for the IT and AT divisions.

Campus Response

The CTC working group referred to in Campus Response #5 will be tasked with developing and implementing a comprehensive plan for periodic testing of IT and AT division DRPs.

Estimated completion: April 30, 2012
October 26, 2011

MEMORANDUM

TO: Mr. Larry Mandel  
University Auditor

FROM: Charles B. Reed  
Chancellor

SUBJECT: Draft Final Report 11-32 on IT Disaster Recovery,  
San Francisco State University

In response to your memorandum of October 26, 2011, I accept the response as submitted with the draft final report on IT Disaster Recovery, San Francisco State University.

CBR/amd