DATA CENTER OPERATIONS

CALIFORNIA STATE UNIVERSITY, EAST BAY

Audit Report 12-33
September 4, 2012

BOARD OF TRUSTEES

THE CALIFORNIA STATE UNIVERSITY

CONTENTS

APPENDICES

ABBREVIATIONS

BDF	Building Distribution Frame
CIO	Chief Information Officer
CSU	California State University
FISMA	Financial Integrity and State Manager's Accountability Act
ICSUAM	Integrated California State University Administrative Manual
ISO	International Standards Organization
ITS	Information Technology Services
MDF	Main Distribution Frame
OUA	Office of the University Auditor
SAM	State Administrative Manual

EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor (OUA) during the last quarter of 2011, the Board of Trustees, at its January 2012 meeting, directed that *Data Center Operations* be reviewed. The OUA had previously reviewed some aspects of *Data Center Operations* in the 2008 and 2009 audits of *Information Security* and the 2010 and 2011 audits of *IT Disaster Recovery Planning*. The OUA also reviewed *Data Center Operations* in the biennial Financial Integrity and State Manager's Accountability Act (FISMA) audits, the last of which was performed on campus in 2008.

We visited the California State University, East Bay campus from May 14, 2012, through June 8, 2012, 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 controls over data center operations. 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 over data center operations in effect as of June 8, 2012, 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.

Our audit did not examine all controls over data center operations but was designed to assess management controls, increase awareness of the topic, and assess regulatory compliance for significant data center operations categories that are prevalent in the California State University environment.

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.

PHYSICAL SECURITY [7]

Background checks were not performed on all employees who had physical access to the information technology services data center. Also, the data center room did not have a security alarm system. Additionally, physical access to the data center, main distribution frame (MDF), and building distribution frame (BDF) rooms needed improvement. Specifically, the list of personnel with authorized access to the data center, MDF, and BDF rooms was not limited to those whose responsibilities required that they have access, and most of the employees with authorized access to the data center room were given master keys, rather than electronic key cards that would have allowed management to track and monitor when they entered and exited the room. Further, the campus did not have procedures to monitor and review

electronic key card access system reports that record the time, dates, and names of employees entering and exiting the data center room, and it did not follow up on any unusual activity noted in the reports.

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS [11]

Data center operations staff had not been trained on fire safety and the use of fire extinguishers.

EMERGENCY PREPAREDNESS AND TRAINING [12]

Data center room shutdown procedures were not updated, tested, or documented to ensure that the ITS staff could properly recover and restart application systems and hardware in the event of an emergency or disaster.

INTRODUCTION

BACKGROUND

Integrated California State University Administrative Manual (ICSUAM) §8000.0, *Information Security Policy*, dated April 19, 2010, represents the most recent and specific guidance to campuses regarding the security and protection of data center operations. It provides direction for managing and protecting the confidentiality, integrity, and availability of California State University (CSU) information assets and defines the organizational scope of information security throughout the system. Specifically, the policy states that the Board of Trustees is responsible for protecting the confidentiality, integrity, and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

ICSUAM §8000.0 further states that it is the collective responsibility of all users to ensure the confidentiality of information that the CSU must protect from unauthorized access; the integrity and availability of information stored on or processed by CSU information systems; and compliance with applicable laws, regulations, and CSU or campus policies governing information security and privacy protection.

The policy applies to all campuses; central and departmentally managed campus information assets; all users employed by campuses or any other person with access to campus information assets; all categories of information, regardless of the medium in which the information asset is held or transmitted (e.g., physical or electronic); and information technology facilities, applications, hardware systems, and network resources owned or managed by the CSU.

ICSUAM §8080 states that each campus must identify physical areas that must be protected from unauthorized physical access. Such areas include data centers and other locations on the campus where information assets containing protected data are stored. Campuses must protect these limited-access areas from unauthorized physical access while ensuring that authorized users have appropriate access. Campus information assets that access protected data located in public and non-public access areas must be physically secured to prevent theft, tampering, or damage. The level of protection provided must be commensurate with that of identifiable risks. Campuses must review and document physical access rights to campus limited-access areas annually.

State Administrative Manual (SAM) §5330 states that physical security practices prevent unauthorized physical access, damage, and interruption to an agency's assets. Physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take the appropriate physical security measures to provide for: management control of physical access to information assets (including personal computer systems, computer terminals, and mobile devices) by agency staff and outsiders; prevention, detection, and suppression of fires; and prevention, detection, and minimization of water damage and loss or disruption of operational capabilities due to electrical power fluctuations or failure.

SAM §5335 states that agencies are responsible for the management and operation of their information processing facilities. The security program should identify and document the appropriate practices to

ensure the integrity and security of the agency's information assets. SAM §5335 references International Standards Organization 17799 Section 9, Physical and Environmental Security, and National Institute of Standards and Technology Special Publication 800-12 (Chapter 15), along with other standards and guidance criteria.

Historically, data center operations were reviewed by the CSU Office of the University Auditor (OUA) as part of cyclical audits based on the Financial Integrity and State Manager's Accountability Act (FISMA) of 1983, passed by the California Legislature and detailed in Government Code §13400 through §13407. Beginning in calendar year 2010, cyclical FISMA audits were reevaluated and discontinued due to a change in the OUA audit risk assessment methodology. Using the new procedure, the OUA worked with CSU campus executive management to identify high-risk areas on each campus. Data Center Operations was selected as a high-risk area to review in 2012.

PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration and control of data center operations; determine the adequacy of controls over the related processes; and ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the overall audit objective, specific goals included determining whether:

- Certain essential administrative and managerial internal controls are in place, including delegations of authority and responsibility, management committees, and documented policies and procedures.
- Data processing facilities employ physical security safeguards for achieving and maintaining appropriate protection of organizational assets.
- Data processing facilities contain adequate fire supression provisions and employ controls that help maintain a proper operating environment.
- Handling procedures for backup media ensure that the movement and storage of tapes is controlled and accountable.
- Formal event reporting and escalation procedures are in place for job scheduling.
- Change management procedures are sufficient to ensure that modifications to the systems or network are authorized.
- Management review of help desk activities ensures a proactive approach toward determining whether there is a systemic cause to problems reported.

SCOPE AND METHODOLOGY

The proposed scope of the audit as presented in Attachment A, Audit Agenda Item 2 of the January 24 and 25, 2012, meeting of the Committee on Audit stated that *Data Center Operations* would include review and compliance with Trustee policy, federal and state directives, and campus policies and procedures; physical security provisions; environmental controls; processing and scheduling controls; backup and recovery processes; and emergency preparations.

Our study and evaluation were 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 currently in effect.

We focused primarily upon the administrative, compliance, operational, and technical controls over the campus data center, network rooms, and personnel operations. Specifically, we reviewed and tested:

- Data center policies and procedures.
- Computer operations organizational structure and management framework.
- Physical security over data processing facilities.
- Fire prevention and environmental controls.
- Emergency preparedness and training.
- Storage and handling of backup media.
- Job scheduling.
- Change management.
- Help desk support.

Our testing and methodology was designed to provide a managerial-level review of key data processing practices over data center operations. Our review did not examine all categories of computer operations; selected IT processes not related to the data center or related data processing facilities were excluded from the scope of the review. Our testing approach was designed to provide a view of the security and controls used to protect only key computing and business processes.

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

PHYSICAL SECURITY

BACKGROUND CHECKS

Background checks were not performed on all employees who had physical access to the information technology services (ITS) data center.

Integrated California State University Administrative Manual (ICSUAM) §8030, *Personnel Information Security*, dated April 19, 2010, states that campuses must develop procedures to conduct background checks on positions involving access to level one information assets as defined in the CSU Data Classification Standard.

Campus ITS Information Security Policy, *Human Resource Security*, revised March 2009, states in part that prior to hiring a new employee, the manager should carefully screen and check the backgrounds of those who will have access to critical assets or confidential/sensitive information. Appropriate background verification checks ("screening") should be carried out by hiring managers under the guidance of an appropriate administrative office (e.g., Human Resources, Academic Affairs, University Police Department, Student Health Services, or the Procurement Office).

The director of server operations services stated that prior to April 2012, background checks were recommended rather than mandatory in the hiring process for ITS personnel. He also stated that a campus executive directive requiring mandatory background checks for all new ITS employees was not issued until April 16, 2012.

Failure to screen and perform background checks on personnel who have access to sensitive data increases the risk of potential mishandling and inappropriate disclosure of sensitive data.

Recommendation 1

We recommend that the campus ensure that background checks are performed on all employees who have physical access to the ITS data center.

Campus Response

We agree. Pursuant to CSU East Bay University Directive Order #11-09, dated April 16, 2012, all "security sensitive positions" receive criminal records checks as part of the human resources new-hire process. This includes custodial staff, University Police department, and information technology job applicants under final consideration for employment at CSU East Bay.

In addition, information technology management will identify information technology employees hired prior to April 16, 2012, who have physical access to the data center, and determine whether their current job duties require continued access. If not, their access to the data center will be curtailed.

ALARM SYSTEM

The data center room did not have a security alarm system.

ICSUAM §8080, *Physical Security*, dated April 19, 2010, states that each campus must identify physical areas that must be protected from unauthorized physical access. Such areas would include data centers and other locations on the campus where information assets containing protected data are stored.

State Administrative Manual (SAM) §5330 states that physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take appropriate physical security measures to provide for control of physical access to information assets by agency staff and outsiders.

The director of server operations services stated that a risk benefit analysis during a time of ITS budget constraints showed the current security arrangement to be sufficient for the new data center, as it featured security access restrictions, as well as cameras inside the room. He also stated that the campus police patrolled the facilities 24 hours a day, seven days a week.

Failure to detect unauthorized entry to the server room increases the risk of security breaches and theft of computing equipment.

Recommendation 2

We recommend that the campus install a security alarm system in the data center room.

Campus Response

We agree. The campus has requested the vendor to re-program the existing security/intrusion alarm system to go to the data center room on a separate feed. The data center alarm will be monitored off-site 24/7 by Siemens Industries, and the alarm will route directly to the campus police department. The estimated completion date is January 31, 2013.

PHYSICAL ACCESS

Physical access to the data center, main distribution frame (MDF), and building distribution frame (BDF) rooms needed improvement. Specifically, we found that:

- The list of personnel with authorized access to the data center, MDF, and BDF rooms was not limited to those whose responsibilities required that they have access. The list included 13 campus police officers, 32 facilities management employees, and 27 ITS employees.

- Most of the employees with authorized access to the data center room were given master keys, rather than electronic key cards that would have allowed management to track and monitor when they entered and exited the room.

ICSUAM §8080, *Physical Security*, dated April 19, 2010, states that each campus must identify physical areas that must be protected from unauthorized physical access. Such areas would include data centers and other locations on the campus where information assets containing protected data are stored.

SAM §5330 states that physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take appropriate physical security measures to provide for control of physical access to information assets by agency staff and outsiders.

Campus ITS Information Security Policy, *Access to the Data Center,* revised March 2009, states that the data center must be locked at all times. Only those university employees whose responsibilities require that they have access to the data center should have credentials to enter. Access to the data center is permitted to other university personnel, business associates, or escorted visitors when such entrance is authorized by the chief information officer (CIO) or information security officer (ISO).

The director of server operations services stated that giving employees master keys to the data center was determined to be an acceptable risk, as employees left their master keys on the premises and did not take them home. He further stated that the number of employees with master keys was small, and the process to issue master keys required authorization from several levels of management.

Failure to provide adequate physical security over information technology assets and sensitive data information increases the risk that unauthorized personnel will have access to information assets and that the campus will not have the capability to track the date and time of personnel entering and exiting the rooms.

Recommendation 3

We recommend that the campus:

a. Evaluate the list of employees with authorized access to the data center, MDF, and BDF rooms to ensure that it is limited to only those whose responsibilities require access.

b. Issue electronic key cards to all personnel authorized to enter the data center room, so that management can track and monitor when they enter and exit the room.

Campus Response

We agree.

a. Management will evaluate the list of employees with authorized access to the data center, MDF, and BDF rooms to ensure that it is limited to only those whose responsibilities require access.

b. Electronic key cards will be issued to all personnel who are authorized to enter the data center room. There will be card readers where personnel enter and exit the data center room.

This will be completed by October 31, 2012.

MONITORING

The campus did not have procedures to monitor and review electronic key card access system reports that record the time, dates, and names of employees entering and exiting the data center room, and it did not follow up on any unusual activity noted in the reports.

ICSUAM §8080, *Physical Security*, dated April 19, 2010, states that each campus must identify physical areas that must be protected from unauthorized physical access. Such areas would include data centers and other locations on the campus where information assets containing protected data are stored.

SAM §5330 states that physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take appropriate physical security measures to provide for control of physical access to information assets by agency staff and outsiders.

Campus ITS Information Security Policy, *Access to the Data Center*, revised March 2009, states that the person supervising the data center must identify any individual not known and refuse entrance to anyone not authorized unless permission is granted by the CIO or ISO.

The director of server operations services stated that the previous operations manager had informally reviewed the authorized personnel list semiannually. He further stated that the issuance of the key cards was limited and went through the same authorization protocols as those for master key holders.

Failure to monitor the electronic security system for personnel entering and exiting the data center room may increase the risk of unusual or inappropriate activity occurring without detection.

Recommendation 4

We recommend that the campus develop and implement procedures to monitor and review the electronic key card access system reports that record the time, dates, and names of employees entering and exiting the data center room, and follow up on any unusual activity noted.

Campus Response

We agree. The director of server operations services will develop and implement procedures to monitor and review the electronic key card access system reports. This will occur on a monthly basis, beginning with September 2012 activity. Any unusual activity will be followed up by the director of server operations services.

The campus will also install a second electronic key card reader at the hallway interior to the data center. The software will be set to "anti-pass-back," meaning that if someone follows another employee out ("piggy-backing"), without using his own card, he will not be able to re-enter the area. Persons entering the area will need to "card in" and "card out"; otherwise, a horn will sound and the user's card will not allow him back into the area. Use of a master key to enter or exit the area will also set off the horn.

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

Data center operations staff had not been trained on fire safety and the use of fire extinguishers.

SAM §5330 states that physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility. Agencies must take appropriate physical security measures to provide for prevention, detection, and suppression of fires.

Campus ITS Information Security Policy, *Access to the Data Center,* revised March 2009, states that the main data center should use a combination of countermeasures (e.g., fire prevention, detection, suppression, and warning systems) to provide protection against natural, environmental, or accidental disasters.

The director of server operations services stated that data center staff had not been trained because the campus had not conducted fire extinguisher training recently. He further stated that training has been scheduled for the data center operations center staff for July 2012.

Failure to provide staff training on fire safety and the use of fire extinguishers increases the risk that information assets will be damaged during minor and preventable fire/combustible accidents.

Recommendation 5

We recommend that the campus provide periodic training to the data center operations staff on fire safety and the use of fire extinguishers.

Campus Response

We agree. We will arrange to have data center staff trained on fire safety and the use of fire extinguishers by November 30, 2012.

In addition, a fire suppression alarm system has been installed in the data center and is monitored off-site by Siemens Industries on a 24/7 basis.

EMERGENCY PREPAREDNESS AND TRAINING

Data center room shutdown procedures were not updated, tested, or documented to ensure that the ITS staff could properly recover and restart application systems and hardware in the event of an emergency or disaster.

ICSUAM §8085, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states that an information security program needs to support the maintenance and potential restoration of operations through and after both minor and catastrophic disruptions. Campuses must ensure that their information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users.

SAM §5330 states, in part, that each agency should ensure the appropriate steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the agency has the ability to continue its essential functions during a business disruption.

Campus ITS Information Security Policy, *Business Continuity*, revised March 2009, states that the university must develop and maintain a business continuity plan that ensures the continuity of essential functions or operations following or during the recovery phase of a catastrophic event.

The director of server operations services stated that attrition in personnel and management, as well as the reorganization that resulted because of such events, caused the process to lapse; however, most of the systems that are on the shutdown sequence, and the order in which they are listed, are still valid.

Failure to maintain a current, tested, and documented shutdown procedure as part of an emergency procedure or disaster recovery can result in unnecessary financial and non-financial losses in the event of an emergency or disaster and could significantly impact the campus' ability to recover data processing services.

Recommendation 6

We recommend that the campus update, test, and document the data center room shutdown procedures to ensure that the ITS staff can properly recover and restart application systems and hardware in the event of an emergency or disaster.

Campus Response

We agree. We will update the March 2009 data center shutdown sequence process document to better reflect changes in the information technology systems infrastructure and revise both the business continuity plan and disaster recovery plan, where applicable, to reflect the revised procedures. The estimated completion date for the revised documentation is December 21, 2012.

However, note that information technology staff is well-versed in performing system shutdowns and performing migrations of virtual systems and have designed resilience in its platform architecture. This was recently demonstrated during the migration of the data center from Warren Hall to its new location.

Current disaster recovery procedures involve the recovery of systems through restoration of service utilizing tape media that is stored off-site. These and other measures employed for disaster recovery will be examined and revised with the campus' disaster recovery plan revision project, which is scheduled to start in winter 2012 and be completed by February 28, 2013.

APPENDIX A:
PERSONNEL CONTACTED

Name	Title
Leroy M. Morishita	President
Rich Avila	Director, Server and Network Operations
Lee Breitzman	Lead Operations Specialist, Server Operations
Matt Collins	Director, Application Systems
Chris Da Silva	Network Analyst
Maggie Graney	Director, Compliance and Internal Control
Jim Hodges	Chief of Police
Audrey Katzman	Information Technology Business Manager
Gene Lim	Director, Server Operations Services
David Miller	Maintenance Manager, Facilities Management
Setareh Sarrafan	Director of User Support Services
Borre Ulrichsen	Deputy Chief Information Officer
Brad Wells	Vice President and Chief Financial Officer, Administration and Finance

CALIFORNIA STATE UNIVERSITY
EAST BAY

Office of the Vice President, Administration and Finance & Chief Financial Officer
CALIFORNIA STATE UNIVERSITY, EAST BAY
25800 Carlos Bee Boulevard, Hayward, CA 94542-3002
510.885-3803 · 510.885.4745 (fax) www.csueastbay.edu

November 15, 2012

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

RE: Campus Response to Data Center Operations Draft Audit
Audit Report Number 12-33
California State University, East Bay

Dear Mr. Mandel,

In response to the review comments sent by Greg Dove on October 29, 2012, the campus has revised our response to the *Data Center Operations* Incomplete Draft Audit Report Number 12-33. This is being electronically transmitted, as requested by your office.

In regard to recommendation #2 on the alarm system, the campus has requested the vendor to re-program the existing intrusion alarm system to go to the Data Center on a separate feed. The audit draft response has been revised accordingly, with estimated dates of completion added for audit recommendations #2, #5 and #6.

Please let us know if you have any questions or need additional information.

Sincerely,

Bradley Wells
Vice President
Administration & Finance, CFO

Attachment

cc: Leroy M. Morishita, President
Maggie Graney, Director of Compliance and Internal Control

DATA CENTER OPERATIONS

CALIFORNIA STATE UNIVERSITY, EAST BAY

Audit Report 12-33

PHYSICAL SECURITY

BACKGROUND CHECKS

Recommendation 1

We recommend that the campus ensure that background checks are performed on all employees who have physical access to the ITS data center.

Campus Response

We agree. Pursuant to CSU East Bay University Directive Order #11-09 from the president, dated April 16, 2012, all "security sensitive positions" receive criminal records checks as part of the human resources new-hire process. This includes custodial staff; University Police department; and Information Technology job applicants under final consideration for employment at CSU East Bay.

In addition, IT management will identify IT employees hired prior to April 16, 2012, who have physical access to the data center, and determine whether their current job duties require continued access. If not, their access to the data center will be curtailed.

ALARM SYSTEM

Recommendation 2

We recommend that the campus install a security alarm system in the data center room.

Campus Response

We agree. The campus has requested the vendor to re-program the existing security/intrusion alarm system to go to the data center room on a separate feed. The data center alarm will be monitored off-site 24/7 by Siemens Industries, and the alarm will route directly to the campus Police department. The estimated completion date is January 31, 2013.

PHYSICAL ACCESS

Recommendation 3

We recommend that the campus:

a. Evaluate the list of employees with authorized access to the data center, MDF, and BDF rooms to ensure that it is limited to only those whose responsibilities require access.

b. Issue electronic key cards to all personnel authorized to enter the data center room, so that management can track and monitor when they enter and exit the room.

Campus Response

a. We agree. Management will evaluate the list of employees with authorized access to the data center, MDF and BDF rooms to ensure that it is limited to only those whose responsibilities require access.

b. We agree. Electronic key cards will be issued to all personnel who are authorized to enter the data center room. There will be card readers where personnel enter and exit the data center room. This will be completed by October 31, 2012.

MONITORING

Recommendation 4

We recommend that the campus develop and implement procedures to monitor and review the electronic key card access system reports that record the time, dates, and names of employees entering and exiting the data center room, and follow up on any unusual activity noted.

Campus Response

We agree. The director of server operations services will develop and implement procedures to monitor and review the electronic key card access system reports. This will occur on a monthly basis, beginning with September 2012 activity. Any unusual activity will be followed up by the director of server operations services.

The campus will also install a second electronic key card reader at the hallway interior to the data center. The software will be set to "anti-pass-back," meaning that if someone follows another employee out ("piggy-backing"), without using his own card, he will not be able to re-enter the area. Persons entering the area will need to 'card in' and 'card out'; otherwise a horn will sound and the user's card will not allow him back into the area. Use of a master key to enter or exit the area will also set off the horn.

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

Recommendation 5

We recommend that the campus provide periodic training to the data center operations staff on fire safety and the use of fire extinguishers.

Campus Response

We agree. We will arrange to have data center staff trained on fire safety and the use of fire extinguishers by November 30, 2012.

In addition, a fire suppression alarm system has been installed in the data center and is monitored off-site by Siemens Industries on a 24/7 basis.

EMERGENCY PREPAREDNESS AND TRAINING

Recommendation 6

We recommend that the campus update, test, and document the data center room shutdown procedures to ensure that the ITS staff can properly recover and restart application systems and hardware in the event of an emergency or disaster.

Campus Response

We agree. We will update the March 2009 data center shutdown sequence process document to better reflect changes in the IT systems infrastructure and revise both the business continuity plan and disaster recovery plan, where applicable, to reflect the revised procedures. The estimated completion date for the revised documentation is December 21, 2012.

However, note that IT staff is well versed in performing system shutdowns and performing migrations of virtual systems, and have designed resilience in its platform architecture. This was recently demonstrated during the migration of the data center from Warren Hall to its new location.

Current disaster recovery procedures involve the recovery of systems through restoration of service utilizing tape media that is stored off-site. These and other measures employed for disaster recovery will be examined and revised with the campus' disaster recovery plan revision project, which is scheduled to start in winter 2012, and be completed by February 28, 2013.

THE CALIFORNIA STATE UNIVERSITY

OFFICE OF THE CHANCELLOR

BAKERSFIELD
CHANNEL ISLANDS
CHICO
DOMINGUEZ HILLS
EAST BAY
FRESNO
FULLERTON
HUMBOLDT
LONG BEACH
LOS ANGELES
MARITIME ACADEMY
MONTEREY BAY
NORTHRIDGE
POMONA
SACRAMENTO
SAN BERNARDINO
SAN DIEGO
SAN FRANCISCO
SAN JOSÉ
SAN LUIS OBISPO
SAN MARCOS
SONOMA
STANISLAUS

December 3, 2012

MEMORANDUM

TO: Mr. Larry Mandel
University Auditor

FROM: Charles B. Reed
Chancellor

SUBJECT: Draft Final Report 12-33 on *Data Center Operations*, California State University, East Bay

In response to your memorandum of December 3, 2012, I accept the response as submitted with the draft final report on *Data Center Operations*, California State University, East Bay.

CBR/amd

401 GOLDEN SHORE • LONG BEACH, CALIFORNIA 90802-4210 • (562) 951-4700 • Fax (562) 951-4986 • creed@calstate.edu