DATA CENTER OPERATIONS
CALIFORNIA STATE UNIVERSITY,
LONG BEACH

Audit Report 12-32
July 24, 2012

Members, Committee on Audit

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

Staff

University Auditor: Larry Mandel
Senior Director: Michael Caldera
IT Audit Manager: Greg Dove
Senior Auditor: Gordon Eng

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
CONTENTS

Executive Summary ...................................................................................................................................... 1

Introduction ................................................................................................................................................... 3
  Background .............................................................................................................................................. 3
  Purpose ..................................................................................................................................................... 5
  Scope and Methodology .......................................................................................................................... 6

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Physical Security ........................................................................................................................................... 7
  Background Checks ................................................................................................................................. 7
  Physical Access ........................................................................................................................................ 7
  Alarm System ........................................................................................................................................ 8

Fire Protection and Environmental Controls .............................................................................................. 9
  Fire Protection .......................................................................................................................................... 9
  Environmental Controls ......................................................................................................................... 10

Emergency Preparedness and Training ....................................................................................................... 11

Operations, Change Control, and Help Desk .............................................................................................. 11
  Networking ............................................................................................................................................ 11
  Firewalls ................................................................................................................................................. 12
APPENDICES

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

ABBREVIATIONS

ATS  Academic Technology Services
AVP  Associate Vice President
CSU  California State University
FISMA Financial Integrity and State Manager’s Accountability Act
ICSUAM Integrated California State University Administrative Manual
ITS  Information Technology Services
MDF  Main Distribution Frame
NIST National Institute of Standards and Technology
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 2006.

We visited the California State University, Long Beach campus from March 26, 2012, through April 20, 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 April 20, 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 (ITS) data center. In addition, the doors to the data centers and network main distribution frame (MDF) room were not equipped with an electronic security system to track and monitor personnel entering and exiting the facilities. Further, the primary campus network MDF room had no security alarm system.
FIRE PROTECTION AND ENVIRONMENTAL CONTROLS [9]

Fire protection measures taken at campus data centers needed improvement. Specifically, the ITS and academic technology services (ATS) data centers and the network MDF room did not have automatic fire suppression systems, and potentially combustible paper materials were stored in the room adjacent to the ITS data center. Also, there were no water sensors in the ATS data center room.

EMERGENCY PREPAREDNESS AND TRAINING [11]

The ITS and ATS data center rooms did not have backup generators capable of sustaining computer operations in the event of a power outage.


The configuration of the external network connections were inadequate to provide disaster redundancy, as both fed into the same campus access point. In addition, the campus had not installed a firewall between the ATS data center systems and the core campus network.
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.
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 suppression 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 Human Resource Policy, Criminal Records Check, dated May 2009, states in part that a criminal records check should be obtained for positions with physical or administrative access to critical information systems.

The associate vice president (AVP) for human resources management stated that the failure to perform background checks was due to oversight and that the existing policy was not consistently followed for temporary employees.

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 concur. The campus will ensure that background checks are performed on all employees who have physical access to the ITS data center. Corrective action on this item is complete.

PHYSICAL ACCESS

The doors to the data centers and network main distribution frame (MDF) room were not equipped with an electronic security system to track and monitor personnel entering and exiting the facilities.

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 AVP for ITS stated that the electronic lock and key systems had not been pursued by ITS or academic technology services (ATS) due to the high cost of installation. She further stated that ITS and ATS follow established university key issuance policy, using state-issued restricted blank keys clearly stamped “do not duplicate.”

Failure to provide an electronic security system 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 2**

We recommend that the campus evaluate the feasibility of installing an electronic security system on data center and MDF room doors that provides the capability to monitor personnel entering and exiting the facilities.

**Campus Response**

We concur. The campus will evaluate the feasibility of installing an electronic security system on data center and MDF room doors. Estimated date of completion is December 31, 2012.

**ALARM SYSTEM**

The primary campus network MDF room had no 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.

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 AVP for ITS stated that security alarms had not been installed in the MDF room due to installation and monitoring costs. In addition, she stated that frequent entry and work performed in the MDF building increased the likelihood of false security alarms, and that existing video cameras were on the same network as the campus video cameras monitored by the campus police department as part of the security service provided to the campus. Also, she stated that although they are not continually monitored, the images are recorded and stored for 21 days. Finally, she stated that the
cameras auto-detect activity in the MDF after regular business hours and on weekends, and if there is activity, the cameras send an alert to the campus police camera monitoring console, where the activity may be viewed by university police.

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

**Recommendation 3**

We recommend that the campus evaluate the feasibility of installing a security alarm system in the primary campus network MDF room.

**Campus Response**

We concur. The campus will evaluate the feasibility of installing a security alarm system in the primary campus network MDF room. Estimated date of completion is December 31, 2012.

**FIRE PROTECTION AND ENVIRONMENTAL CONTROLS**

**FIRE PROTECTION**

Fire protection measures taken at campus data centers needed improvement.

We found that:

- The ITS and ATS data centers and the network MDF room did not have automatic fire suppression systems.

- Potentially combustible paper materials were stored in the room adjacent to the ITS data center.

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.

The AVP for ITS stated that the campus was following the National Institute of Standards and Technology standard, which states that fire extinguishment can be performed by people using portable extinguishers. Also, she stated that the copy/printing paper was stored in a room next to the ITS data center in order to condition or acclimatize the paper prior to its use, and alternative storage locations were not available due to limited space on campus. Further, she stated that the State Fire Marshal performed a regular inspection of the area subsequent to the audit and did not find the paper storage to be in violation with state fire regulations.
Failure to provide an automatic fire suppression system increases the risk that information assets will be damaged during disasters or emergencies, and the practice of storing combustible materials within the surrounding areas can worsen conditions in a fire.

**Recommendation 4**

We recommend that the campus evaluate the feasibility of:

a. Installing automatic fire suppression systems in the ITS and ATS data centers and the network MDF room.

b. Moving the potentially combustible paper materials to another climate-controlled location.

**Campus Response**

We concur. The campus acknowledges and accepts the risk of not having automatic fire suppression systems in the ITS and ATS data centers and the network MDF room. The campus also acknowledges and accepts the risk of storing potentially combustible paper materials in the ITS data center. According to the State Fire Marshal, the location of these paper materials in the data center is not in violation of state fire regulations.

**ENVIRONMENTAL CONTROLS**

There were no water sensors in the ATS data center room.

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 minimization of water damage.

The interim AVP of ATS and dean and director of the University Library stated that water sensors in the ATS data center had not been installed because flooding was not a known risk for the location due to the general topography of the area, which is an elevated site compared to the rest of the campus.

Failure to detect and prevent water or flooding in the data center room can result in damaged information assets.

**Recommendation 5**

We recommend that the campus evaluate the feasibility of installing a water sensor in the ATS data center room.
Campus Response

We concur. The campus will evaluate the feasibility of installing a water sensor in the ATS data center room. Estimated date of completion is December 31, 2012.

EMERGENCY PREPAREDNESS AND TRAINING

The ITS and ATS data center rooms did not have backup generators capable of sustaining computer operations in the event of a power outage.

ICSUAM §8085, Business Continuity and Disaster Recovery, dated April 19, 2010, states that each campus must ensure that information assets can, in case of a catastrophic event, continue to operate and be appropriately accessible to users.

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 minimization of loss or disruption of operational capabilities due to electrical power fluctuations or failure.

The AVP for ITS stated that ITS and ATS had not purchased or installed backup generators due to the extremely high cost.

The lack of backup generators capable of sustaining computer operations increases the risk that the campus could lose the ability to provide data processing services in the event of a power outage, which could disrupt campus operations.

Recommendation 6

We recommend that the campus install backup generators in the ITS and ATS data center rooms capable of sustaining computer operations in the event of campus power outage.

Campus Response

We concur. The campus acknowledges and accepts the risk of not having backup generators in the ITS and ATS data center rooms.

OPERATIONS, CHANGE CONTROL, AND HELP DESK

NETWORKING

The configuration of the external network connections were inadequate to provide disaster redundancy, as both fed into the same campus access point.
ICSUAM §8085, *Business Continuity and Disaster Recovery*, dated April 19, 2010, states that each campus must ensure that information assets can, in case of a catastrophic event, continue to operate and be appropriately accessible to users.

The AVP for ITS stated that the campus and the chancellor’s office were aware of the lack of network redundancy at Long Beach and other campuses. She further stated that addressing the lack of redundancy at the campus level was not financially feasible, but a plan to provide network redundancy and increased bandwidth to and from Cenic had been established as part of the CSU Network Initiative. She also stated that the Long Beach campus was not selected as one of the first group of campuses to be upgraded, and therefore she did not know the timing for the campus upgrade within the chancellor’s office plan.

Lack of an adequate backup configuration increases the risk that the campus could lose the ability to communicate externally in the event of a disaster at the MDF, which could disrupt campus operations.

**Recommendation 7**

We recommend that the campus evaluate the feasibility of reconfiguring the campus’ external network connections so that they feed into separate campus access points.

**Campus Response**

We concur. We will contact the chancellor’s office to request that California State University, Long Beach be added to the Cenic infrastructure upgrade initiative. Corrective action on this item is complete.

**FIREWALLS**

The campus had not installed a firewall between the ATS data center systems and the core campus network.

ICSUAM §8045, *Information Technology Security*, dated April 19, 2010, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

The interim AVP for ATS and dean and director of the University Library stated that the ATS data center had not been firewalled from the campus network due to resource constraints.

Failure to create a firewall between a secondary data center room and the core campus network increases the risk that unauthorized or illegitimate network traffic may gain access to and compromise the primary data center’s information assets and sensitive data.
Recommendation 8

We recommend that the campus install a firewall between the ATS data center systems and the core campus network.

Campus Response

We concur. Due to resource and time constraints, moving the servers behind the campus firewall will occur in stages. A project plan will be created to move all ATS mission critical servers with level 1 and level 2 data. Estimated date of completion is January 31, 2013.

The most critical server, the Library Management System server, will be moved behind the campus firewall. Estimated date of completion is January 31, 2013.

All new servers will be placed behind the campus firewall before they are put in production.
# APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>F. King Alexander</td>
<td>President</td>
</tr>
<tr>
<td>Martha Carey</td>
<td>Data Center Operator</td>
</tr>
<tr>
<td>Janet Foster</td>
<td>Associate Vice President, Information Technology Services (ITS)</td>
</tr>
<tr>
<td>Vickie Hamilton</td>
<td>Director, Human Resources</td>
</tr>
<tr>
<td>Byron Jackson</td>
<td>Director of Service Management and Operations, ITS</td>
</tr>
<tr>
<td>Craig Kleen</td>
<td>Assistant Director of Network Services, ITS</td>
</tr>
<tr>
<td>Roman Kochan</td>
<td>Interim Associate Vice President of Academic Technology Services (ATS) and Dean and Director, University Library</td>
</tr>
<tr>
<td>Steve La</td>
<td>Director of Network, Telecommunication and Security, ITS</td>
</tr>
<tr>
<td>Michael Markoski</td>
<td>Director of Data Center and Emergency Management, ITS</td>
</tr>
<tr>
<td>Greg Pascal</td>
<td>Communications/Information System Manager, University Police</td>
</tr>
<tr>
<td>Cheryl Perkins</td>
<td>Administrative Services Manager</td>
</tr>
<tr>
<td>Wayne Pierson</td>
<td>Director of Servers, Systems and Websites, ITS</td>
</tr>
<tr>
<td>Aysu Spruill</td>
<td>Director of Internal Auditing/Information Security Officer</td>
</tr>
<tr>
<td>Mary Stephens</td>
<td>Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Ryan Tapp</td>
<td>Library, Desktop and User Support, ATS</td>
</tr>
<tr>
<td>Don Taylor</td>
<td>Operating Systems Technical Lead, ITS Servers, Systems and Web</td>
</tr>
</tbody>
</table>
August 23, 2012

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

Re: Response to Data Center Audit #12-32

Dear Larry:

Please find enclosed California State University, Long Beach's response to the above report. The campus is committed to addressing and resolving the issues identified in the audit report.

Please let me know if we can provide you with any additional information.

Sincerely,

F. King Alexander
President

Enclosure

IA-0301

c: Scott Apel, Associate Vice President, Human Resources Management
   Janet Foster, Associate Vice President, Information Technology Services
   Jill Horn, Director, Technology Support Services
   Ted Kadowaki, Associate Vice President, Budget and University Services
   Roman Kochan, Interim Associate Vice President of Academic Technology Services
   Donald Para, Provost and Senior Vice President Academic Affairs
   Aysu Spruill, Director, Internal Auditing Services/Information Security Officer
   Mary Stephens, Vice President for Administration and Finance
DATA CENTER OPERATIONS

CALIFORNIA STATE UNIVERSITY,
LONG BEACH

Audit Report 12-32

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 concur. The campus will ensure that background checks are performed on all employees who have physical access to the ITS data center. Corrective action on this item is complete.

PHYSICAL ACCESS

Recommendation 2

We recommend that the campus evaluate the feasibility of installing an electronic security system on data center and MDF room doors that provides the capability to monitor personnel entering and exiting the facilities.

Campus Response

We concur. The campus will evaluate the feasibility of installing an electronic security system on data center and MDF room doors. Estimated date of completion is December 31, 2012.

ALARM SYSTEM

Recommendation 3

We recommend that the campus evaluate the feasibility of installing a security alarm system in the primary campus network MDF room.

Campus Response

We concur. The campus will evaluate the feasibility of installing a security alarm system in the primary campus network MDF room. Estimated date of completion is December 31, 2012.
FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

FIRE PROTECTION

Recommendation 4

We recommend that the campus evaluate the feasibility of:

a. Installing automatic fire suppression systems in the ITS and ATS data centers and the network MDF room.

b. Moving the potentially combustible paper materials to another climate-controlled location.

Campus Response

We concur. The campus acknowledges and accepts the risk of not having automatic fire suppression systems in the ITS and ATS data centers and the network MDF room. The campus also acknowledges and accepts the risk of storing potentially combustible paper materials in the ITS data center. According to the State Fire Marshal, the location of these paper materials in the data center is not in violation of state fire regulations.

ENVIRONMENTAL CONTROLS

Recommendation 5

We recommend that the campus evaluate the feasibility of installing a water sensor in the ATS data center room.

Campus Response

We concur. The campus will evaluate the feasibility of installing a water sensor in the ATS data center room. Estimated date of completion is December 31, 2012.

EMERGENCY PREPAREDNESS AND TRAINING

Recommendation 6

We recommend that the campus install backup generators in the ITS and ATS data center rooms capable of sustaining computer operations in the event of campus power outage.

Campus Response

We concur. The campus acknowledges and accepts the risk of not having backup generators in the ITS and ATS data center rooms.
OPERATIONS, CHANGE CONTROL, AND HELP DESK

NETWORKING

Recommendation 7

We recommend that the campus evaluate the feasibility of reconfiguring the campus’ external network connections so that they feed into separate campus access points.

Campus Response

We concur. We will contact the chancellor’s office to request that CSULB be added to the Cenic infrastructure upgrade initiative. Corrective action on this item is complete.

FIREWALLS

Recommendation 8

We recommend that the campus install a firewall between the ATS data center systems and the core campus network.

Campus Response

We concur. Due to resource and time constraints, moving the servers behind the campus firewall will occur in stages. A project plan will be created to move all ATS mission critical servers with level 1 and level 2 data. Estimated date of completion is January 31, 2013.

The most critical server, the Library Management System server, will be moved behind the campus firewall. Estimated date of completion is January 31, 2013.

All new servers will be placed behind the campus firewall before they are put in production.
September 7, 2012

MEMORANDUM

TO: Mr. Larry Mandel  
University Auditor

FROM: Charles B. Reed  
Chancellor

SUBJECT: Draft Final Report 12-32 on Data Center Operations, California State University, Long Beach

In response to your memorandum of September 7, 2012, I accept the response as submitted with the draft final report on Data Center Operations, California State University, Long Beach.

CBR/amd