DATA CENTER OPERATIONS

CALIFORNIA STATE UNIVERSITY,
DOMINGUEZ HILLS

Audit Report 12-31
June 15, 2012

Members, Committee on Audit

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

Staff

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

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
  Data Center Alarm ............................................................................................................................... 7
  Network Closet Security ...................................................................................................................... 7

Fire Protection and Environmental Controls .......................................................................................... 8

Emergency Preparedness and Training .................................................................................................. 9
APPENDICES

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

ABBREVIATIONS

CIO        Chief Information Officer
CSU        California State University
FISMA      Financial Integrity and State Manager’s Accountability Act
ICSUAM     Integrated CSU Administrative Manual
IT          Information 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 2008.

We visited the Dominguez Hills campus from February 20, 2012, through March 9, 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 March 9, 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]

The campus data center was not equipped with a security alarm, and network wiring rooms in certain buildings were not adequately secured to prevent unauthorized access to network switches.

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS [8]

Information technology personnel who worked in and near the data center had not been trained in the operation of the center’s Halon fire suppression system.
EMERGENCY PREPAREDNESS AND TRAINING [9]

The campus did not have documented data center emergency procedures, and disaster instructions were not posted prominently throughout the data center or on the employee bulletin board.
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

DATA CENTER ALARM

The campus data center was not equipped with a security alarm.

Integrated California State University Administrative Manual (ICSUAM) §8080, *Physical Security*, dated April 19, 2010, states that each campus must identify physical areas that must be protected from unauthorized physical access.

California State University, Dominguez Hills *VISC Data Center Physical Control Guideline* states that campus physical controls must be adequate to protect critical or protected data. Such controls must prevent, detect, suppress fire, water damage, and loss or disruption of operational capabilities due to electrical power fluctuations or failure.

The chief information officer (CIO) stated that the computer room has locked doors and external surveillance cameras, and the entire building is locked at night.

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

**Recommendation 1**

We recommend that the campus evaluate the feasibility of installing a security alarm.

**Campus Response**

We concur. The campus has evaluated the feasibility of installing a security alarm system and has made a decision to move forward on the installation of the alarm.

Expected completion date: Completed

NETWORK CLOSET SECURITY

Network wiring rooms in certain buildings were not adequately secured to prevent unauthorized access to network switches.

Specifically, we noted that:

- The network rack in the theater building was located in an open stairwell and was unlocked.
- The network box in the gymnasium was unlocked.
- Several rooms had roof access that was not appropriately secured.
- Two rooms were accessible to janitorial personnel.
ICSUAM § 8080, *Physical Security*, dated April 19, 2010, states that each campus must identify physical areas that must be protected from unauthorized physical access.

California State University, Dominguez Hills *VISC Data Center Physical Control Guideline* states that campus physical controls must be adequate to protect critical or protected data. Such controls must prevent, detect, suppress fire, water damage, and loss or disruption of operational capabilities due to electrical power fluctuations or failure.

The CIO stated that the campus had designed secure network rooms in the newer buildings, but that some of the older locations were shared with campus facility operations, and additional coordination of security requirements was needed.

Failure to prevent unauthorized access to network rooms increases the risk of security breaches and theft of computing equipment.

**Recommendation 2**

We recommend that the campus:

a. Adequately secure the cited network wiring rooms.
b. Evaluate and, if necessary, adequately secure all other network wiring rooms.

**Campus Response**

We concur.

a. The campus will adequately secure the cited network wiring rooms.
b. The campus will evaluate, and if necessary, adequately secure other network wiring rooms.

Expected completion date: October 2012

**FIRE PROTECTION AND ENVIRONMENTAL CONTROLS**

Information technology (IT) personnel who worked in and near the data center had not been trained in the operation of the center’s Halon fire suppression system.

State Administrative Manual (SAM) § 5355.1 states that disaster recovery plans and other IT procedures should be developed to ensure that critical services and applications are restored as quickly as possible and with minimal loss of data.

The CIO stated that the data center environmental systems were maintained and supported by trained facilities personnel.
Failure to train personnel on the data center emergency systems could lead to misunderstanding and confusion in the event of a disaster or emergency.

**Recommendation 3**

We recommend that the campus train IT personnel who work in and near the data center in the operation of the center’s Halon fire suppression system.

**Campus Response**

We concur. The campus has made a conscious decision to continue operations as currently practiced. The IT staff will leave the area in the event of the Halon fire suppression system triggering, leaving the operation of the system to qualified physical plant staff.

Expected completion date: Completed

**EMERGENCY PREPAREDNESS AND TRAINING**

The campus did not have documented data center emergency procedures, and disaster instructions were not posted prominently throughout the data center or on the employee bulletin board.

SAM §5355.1 states that disaster recovery plans and other IT procedures should be developed to ensure that critical services and applications are restored as quickly as possible and with minimal loss of data.

The CIO stated that the data center is normally unattended, and he was unaware of the requirement to post emergency and disaster instructions throughout the center.

Failure to document emergency and disaster instructions and post them prominently could lead to misunderstanding and confusion in the event of a disaster or emergency.

**Recommendation 4**

We recommend that the campus document data center emergency procedures and post them prominently throughout the data center and on the employee bulletin board.

**Campus Response**

We concur. The campus will document data center emergency procedures and post them prominently throughout the data center and on the employee bulletin board.

Expected completion date: October 2012
## APPENDIX A:
### PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Willie Hagan</td>
<td>Interim President (Currently)</td>
</tr>
<tr>
<td>Mildred Garcia</td>
<td>President (At time of review)</td>
</tr>
<tr>
<td>Mahabub Alam</td>
<td>Network Specialist, Campus Backbone Network</td>
</tr>
<tr>
<td>Ron Bergmann</td>
<td>Associate Vice President and Chief Information Officer, Information Technology (IT)</td>
</tr>
<tr>
<td>Ed Laio</td>
<td>Network Analyst</td>
</tr>
<tr>
<td>Danny Lujan</td>
<td>Director of Infrastructure</td>
</tr>
<tr>
<td>Mary Ann Rodriguez</td>
<td>Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Jonathan Scheffler</td>
<td>Associate Director, Physical Plant</td>
</tr>
<tr>
<td>Karen Wall</td>
<td>Associate Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Muneca Williams</td>
<td>IT Administrative Support Assistant</td>
</tr>
</tbody>
</table>
June 28, 2012

Mr. Larry Mandel  
University Auditor  
The California State University  
401 Golden Shore, 4th Floor  
Long Beach, CA  90802-4210  

Dear Mr. Mandel:

Enclosed, please find California State University, Dominguez Hills’ responses to the Data Center Operations Audit Report 12-31, dated June 15, 2012. The campus is committed to addressing and resolving the issues identified in the audit report.

If you have any questions or would like additional information, please contact me.

Sincerely,

Mary Ann Rodriguez  
Vice President, Administration and Finance

Enclosure (1)  
e: Willie Hagan, Interim President  
Karen Wall, Associate Vice President, Administration and Finance
DATA CENTER OPERATIONS
CALIFORNIA STATE UNIVERSITY,
DOMINGUEZ HILLS
Audit Report 12-31

PHYSICAL SECURITY

DATA CENTER ALARM

Recommendation 1

We recommend that the campus evaluate the feasibility of installing a security alarm.

Campus Response

We concur. The campus has evaluated the feasibility of installing a security alarm system and has made a decision to move forward on the installation of the alarm.

Expected completion date: Completed

NETWORK CLOSET SECURITY

Recommendation 2

We recommend that the campus:

a. Adequately secure the cited network wiring rooms.
b. Evaluate and, if necessary, adequately secure all other network wiring rooms.

Campus Response

We concur.

a. The campus will adequately secure the cited network wiring rooms.
b. The campus will evaluate, and if necessary, adequately secure other network wiring rooms.

Expected completion date: October 2012

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

Recommendation 3

We recommend that the campus train IT personnel who work in and near the data center in the operation of the center’s Halon fire suppression system.
Campus Response

We concur. The campus has made a conscious decision to continue operations as currently practiced. The IT staff will leave the area in the event of the Halon fire suppression system triggering leaving the operation of the system to qualified physical plant staff.

Expected completion date: Completed

EMERGENCY PREPARDNESS AND TRAINING

Recommendation 4

We recommend that the campus document data center emergency procedures and post them prominently throughout the data center and on the employee bulletin board.

Campus Response

We concur. The campus will document data center emergency procedures and post them prominently throughout the data center and on the employee bulletin board.

Expected completion date: October 2012
July 19, 2012

MEMORANDUM

TO: Mr. Larry Mandel
   University Auditor

FROM: Charles B. Reed
   Chancellor

SUBJECT: Draft Final Report 12-31 on Data Center Operations,
   California State University, Dominguez Hills

In response to your memorandum of July 19, 2012, I accept the response as
submitted with the draft final report on Data Center Operations, California
State University, Dominguez Hills.

CBR/amd