DATA CENTER OPERATIONS

CALIFORNIA STATE UNIVERSITY,
CHICO

Audit Report 12-35
October 19, 2012

Members, Committee on Audit

Henry Mendoza, Chair
William Hauck, Vice Chair
Lupe C. Garcia  Steven M. Glazer
Hugo N. Morales  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 ................................................................................................................................................... 2
  Background ............................................................................................................................................... 2
  Purpose ...................................................................................................................................................... 4
  Scope and Methodology ........................................................................................................................... 5

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Physical Security ........................................................................................................................................... 6

Fire Protection and Environmental Controls ................................................................................................ 7
APPENDICES

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

ABBREVIATIONS

CSU          California State University
FISMA        Financial Integrity and State Manager’s Accountability Act
ICSUAM       Integrated California State University Administrative Manual
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, Chico campus from July 9, 2012, through August 2, 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 August 2, 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 [6]

The list of personnel with authorized access to the data center rooms was not limited to those whose responsibilities required that they have access.

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS [7]

Campus data center rooms did not have smoke detection systems or automatic fire suppression systems.
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 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.
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.
PHYSICAL SECURITY

The list of personnel with authorized access to the data center rooms was not limited to those whose responsibilities required that they have access.

We found that 38 campus police officers, 23 information resources employees, and six facilities management employees had access cards or master keys to the data center rooms, including the primary, secondary, and co-location data rooms.

Integrated California State University Administrative Manual (ICSUAM) §8030, Personnel Information 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. Campuses must protect these limited-access areas from unauthorized physical access while ensuring that authorized users have appropriate access.

State Administrative Manual (SAM) §5330, Physical and Environmental Security, 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 communication services stated that the campus had determined that the authorization and distribution of key card access was reasonable because the network and telecommunications infrastructure, which requires additional access for network and telecommunications personnel, was located in the primary and secondary data rooms. He further stated that police department access appeared excessive, and they will consider reducing access.

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.

Recommendation 1

We recommend that the campus evaluate the list of employees with authorized access to the data center rooms to ensure that it is limited to only those whose responsibilities require access.

Campus Response

We concur with the recommendation and have already taken action to evaluate and reduce the amount of personnel with access rights to the data center. Corrective action on this item is complete.
FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

Campus data center rooms did not have smoke detection systems or automatic fire suppression systems.

SAM §5330, Physical and Environmental Security, 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 director of communication services stated that the campus had decommissioned an outdated Halon fire suppression system in the primary data center due to environmental reasons and had not installed a replacement system, and that the secondary and co-location data center rooms have never had a fire suppression system.

Failure to provide smoke detection systems and automatic fire suppression systems in data center rooms increases the risk that computing equipment will be damaged during a fire.

Recommendation 2

We recommend that the campus install smoke detection systems and automatic fire suppression systems in the data center rooms.

Campus Response

We concur with the recommendation to install fire suppression systems in the primary data center. The campus has begun the process to mitigate the issue. The fire suppression system on the fourth floor of Butte Hall is a component of a life safety project, new elevators, due to be complete by August 31, 2013.

We concur with the recommendation to install smoke detection systems in the primary and secondary data centers. Installation of smoke detectors for both locations will be complete by August 31, 2013.

The campus will accept the risk associated with lack of a fire suppression system in the Meriam Library, the secondary data center. Since this is a redundant system and the primary system will be adequately protected, the campus will not proceed with the recommended building upgrade at this time.
### APPENDIX A:
**PERSONNEL CONTACTED**

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul J. Zingg</td>
<td>President</td>
</tr>
<tr>
<td>Sharyn Abernatha</td>
<td>Assistant Vice President for Staff Human Resources</td>
</tr>
<tr>
<td>Scott Claverie</td>
<td>Director of Communications Services</td>
</tr>
<tr>
<td>Lee Cummings</td>
<td>Supervisor, Telecommunication Services</td>
</tr>
<tr>
<td>Amy Gremer</td>
<td>Manager of Employment Services</td>
</tr>
<tr>
<td>Lorraine Hoffman</td>
<td>Vice President for Business and Finance</td>
</tr>
<tr>
<td>Ed Hudson</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>Jeni Kitchell</td>
<td>Interim Director of University Budget and Resource Management</td>
</tr>
<tr>
<td>Andrea Mox</td>
<td>Manager, IT Support Services</td>
</tr>
<tr>
<td>Mike Murray</td>
<td>Administrative Desktop Management</td>
</tr>
<tr>
<td>Dennis Partington</td>
<td>Network Manager</td>
</tr>
<tr>
<td>Ray Quinto</td>
<td>Manager, Enterprise Systems</td>
</tr>
<tr>
<td>Ryan Richter</td>
<td>Labs and Academic Desktop Management</td>
</tr>
<tr>
<td>Jerry Ringel</td>
<td>Director, Computing and Technology Support</td>
</tr>
<tr>
<td>Tom Rosenow</td>
<td>Director, Application Development and Technical Support, Enrollment Management</td>
</tr>
<tr>
<td>Michael Schilling</td>
<td>Vice Provost for Information Resources and Chief Information Officer</td>
</tr>
<tr>
<td>Kevin Weherly</td>
<td>Desktop Support Services</td>
</tr>
</tbody>
</table>
December 10, 2012

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

Subject: Data Center Operations, Audit Report 12-35  
California State University, Chico

Dear Mr. Mandel:

We have reviewed the Office of the University Auditor Report 12-35, Data Center Operations at California State University, Chico. Please find enclosed our response to the audit recommendations 1 and 2. Upon acceptance of our response, the campus will submit documentation evidencing implementation of the recommendations.

If you have any questions or require additional information, please contact Jeni Kitchell at 530-898-5910 or jkitchell@csuchico.edu. Thank you.

Sincerely,

[Signature]

Paul J. Zingg  
President

Enclosure

cc: Lorraine Hoffman, Vice President for Business and Finance, CSU Chico  
Michael Schilling, Vice Provost for Information Resources and CIO, CSU Chico  
Jeni Kitchell, CSU Chico

The California State University
DATA CENTER OPERATIONS
CALIFORNIA STATE UNIVERSITY, CHICO
Audit Report 12-35

PHYSICAL SECURITY

Recommendation 1

We recommend that the campus evaluate the list of employees with authorized access to the data center rooms to ensure that it is limited to only those whose responsibilities require access.

Campus Response

We concur with the recommendation and have already taken action to evaluate and reduce the amount of personnel with access rights to the data center. Corrective action on this item is complete.

FIRE PROTECTION AND ENVIRONMENTAL CONTROLS

Recommendation 2

We recommend that the campus install smoke detection systems and automatic fire suppression systems in the data center rooms.

Campus Response

We concur with the recommendation to install fire suppression systems in the primary data center. The campus has begun the process to mitigate the issue. The fire suppression system on the fourth floor of Butte Hall is a component of a life safety project, new elevators, due to complete by August 31, 2013.

We concur with the recommendation to install smoke detection systems in the primary and secondary data centers. Installation of smoke detectors for both locations will be complete by August 31, 2013.

The campus will accept the risk associated with lack of a fire suppression system in the Meriam Library, the secondary data center. Since this is a redundant system and the primary system will be adequately protected, the campus will not proceed with the recommended building upgrade at this time.
January 16, 2013

MEMORANDUM

TO: Mr. Larry Mandel
    University Auditor

FROM: Timothy P. White
    Chancellor

SUBJECT: Draft Final Report 12-35 on *Data Center Operations*,
California State University, Chico

In response to your memorandum of January 16, 2013, I accept the response as submitted with the draft final report on *Data Center Operations*, California State University, Chico.

TPW/amd