

AUXILIARY ORGANIZATIONS
CALIFORNIA STATE UNIVERSITY,
CHICO

Audit Report 09-19
May 6, 2010

Members, Committee on Audit

Henry Mendoza, Chair
Raymond W. Holdsworth, Vice Chair
Nicole M. Anderson Margaret Fortune
George G. Gowgani Melinda Guzman
William Hauck

Staff

University Auditor: Larry Mandel
Senior Director: Janice Mirza
Audit Manager: Gary Miller
Senior Auditors: Kwabena Boakye and Jamarr Johnson
Internal Auditor: Salesian Yuen

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction.....	5
Background	5
Purpose.....	6
Scope and Methodology	7

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

CAMPUS

Information Technology	10
------------------------------	----

THE UNIVERSITY FOUNDATION CALIFORNIA STATE UNIVERSITY, CHICO

Operating and Administrative Agreements	12
Corporate Governance	13
Fees, Revenues and Receivables	14
Endowment Administration.....	14
Information Technology	15
Information Security Training	15
Data Security.....	17

THE CSU, CHICO RESEARCH FOUNDATION

Property and Equipment	18
Trusts and Other Liabilities	19

ASSOCIATED STUDENTS OF CALIFORNIA STATE UNIVERSITY, CHICO

Fiscal Compliance.....	21
Cash Receipts and Handling.....	22
Personnel and Payroll	23

CONTENTS

Information Technology	24
Password Security	24
Data Security	25
Information Security Training and Data Confidentiality Forms	26
User Access Reviews	28
Web Application Security	29
System Backups	30
Disaster Recovery Plan	31
Antivirus Software	32

APPENDICES

APPENDIX A:	Personnel Contacted
APPENDIX B:	Statement of Internal Controls
APPENDIX C:	Campus Response
APPENDIX D:	Chancellor's Acceptance

ABBREVIATIONS

AORMA	Auxiliary Organization Risk Management Authority
AS	Associated Students of California State University, Chico
CSU	California State University
CSUC	California State University, Chico
CSURMA	California State University Risk Management Authority
DRP	Disaster Recovery Plan
EO	Executive Order
IFAS	Integrated Financial and Accounting System
IRS	Internal Revenue Service
IT	Information Technology
MBS	Missouri Book System
PCI DSS	Payment Card Industry Data Security Standard
Research Foundation	The CSU, Chico Research Foundation
RFIN	Resolution of the Committee on Finance
SAQ	Self-Assessment Questionnaire
UBI	Unrelated Business Income
University Foundation	The University Foundation California State University, Chico

EXECUTIVE SUMMARY

In July 1981, the Board of Trustee policy concerning auxiliary organizations was adopted in the Resolution of the Committee on Finance (RFIN) 7-81-4. Executive Order 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, required that the Office of the University Auditor conduct internal compliance/internal control reviews of auxiliary organizations, and the Board of Trustees instructed that such reviews be conducted on a triennial basis pursuant to procedures established by the chancellor.

California State University, Chico (CSUC) management is responsible for establishing and maintaining an adequate system of internal compliance/internal control and assuring that each of its auxiliary organizations similarly establishes such a system. This responsibility, in accordance with California Code of Regulations, Title 5, Section 42402 et seq. and Executive Order 698, *Board of Trustees Policy for The California State University Auxiliary Organizations et seq.*, includes requiring the documentation of internal control, communicating requirements to employees, and assuring that its system of internal compliance/internal control is functioning as prescribed. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of control procedures.

The objectives of a system of internal compliance/internal control are to provide management with reasonable, but not absolute, assurance that:

- ▶ Auxiliary operations are conducted in accordance with policies and procedures established in the State Administrative Manual, Education Code, Title 5, and Trustee policy.
- ▶ Assets are adequately safeguarded against loss from unauthorized use or disposition.
- ▶ Transactions are executed in accordance with management's authorization and recorded properly to permit the timely preparation of reliable financial statements.

We visited the CSUC campus and its auxiliary organizations from November 16, 2009, through December 18, 2009, and made a study and evaluation of the system of internal compliance/internal control in effect as of December 18, 2009. This report represents our triennial review.

Our study and evaluation at *The University Foundation California State University, Chico* revealed certain conditions that, in our opinion, could result in errors and irregularities if not corrected. Specifically, the auxiliary did not maintain adequate control over information technology. These conditions, along with other weaknesses, are described in the executive summary and in the body of the report. In our opinion, except for the effect of the weaknesses described above, accounting and administrative control in effect as of December 18, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *The CSU, Chico Research Foundation* did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. However, we did identify other reportable weaknesses that are described in the executive summary and in the body of the report. In our opinion, the accounting and administrative

control in effect as of December 18, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *Associated Students of California State University, Chico* revealed certain conditions that, in our opinion, could result in errors and irregularities if not corrected. Specifically, the auxiliary did not maintain adequate control over information technology. These conditions, along with other weaknesses, are described in the executive summary and in the body of the report. In our opinion, except for the effect of the weaknesses described above, accounting and administrative control in effect as of December 18, 2009, taken as a whole, was sufficient to meet the objectives stated above.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

The following summary provides management with an overview of conditions requiring their attention. Areas of review not mentioned in this section were found to be satisfactory. Numbers in brackets [] refer to page numbers in the report.

CAMPUS

INFORMATION TECHNOLOGY [10]

The campus did not ensure that the auxiliaries had fully addressed Payment Card Industry Data Security Standard requirements. This is a repeat finding from our Information Security audit conducted in August 2008.

THE UNIVERSITY FOUNDATION CALIFORNIA STATE UNIVERSITY, CHICO

OPERATING AND ADMINISTRATIVE AGREEMENTS [12]

Certain agreements between The University Foundation California State University, Chico (University Foundation) and third-party service providers did not include appropriate indemnification provisions.

CORPORATE GOVERNANCE [13]

The University Foundation had not filed amended Bylaws with the chancellor's office in a timely manner.

FEES, REVENUES, AND RECEIVABLES [14]

University Foundation matching gift procedures did not require that a documented dual review be performed to ensure that funds are administered in accordance with corporate donor requirements.

ENDOWMENT ADMINISTRATION [14]

Certain University Foundation endowment files lacked documented donor intent and scholarship guidelines.

INFORMATION TECHNOLOGY [15]

University Foundation and advancement personnel with access to critical systems or protected data were not required to complete information security awareness training. In addition, protected data stored in the donor system was not encrypted.

THE CSU, CHICO RESEARCH FOUNDATION

PROPERTY AND EQUIPMENT [18]

Dispositions and acquisitions of Research Foundation property and equipment were only communicated to the Research Foundation once annually by campus property management operations, and thus were not processed in a timely manner.

TRUSTS AND OTHER LIABILITIES [19]

The Research Foundation had not completed a review of its custodial trust accounts to determine the source of deposits, and therefore, certain campus program revenues may be inappropriately deposited to, and held in custody by, the Research Foundation.

ASSOCIATED STUDENTS OF CALIFORNIA STATE UNIVERSITY, CHICO

FISCAL COMPLIANCE [21]

Unrelated business income for servicing and repairing of Apple computer equipment provided to the public (non-students) was not accounted for/reported by Associated Students of California State University, Chico (AS).

CASH RECEIPTS AND HANDLING [22]

Accountability for cash receipts at the AS Butte and Holt convenience store locations required improvement, as separate logons and closeout procedures were not used to establish accountability when multiple cashiers used the same cash register, there was a lack of individual cashier accountability for daily cash collections, and there was no daily reconciliation of cash collected to sales register totals.

PERSONNEL AND PAYROLL [23]

The AS payroll system did not generate a report of pay rate changes for management review.

INFORMATION TECHNOLOGY [24]

Password and login security controls were not always adequate for AS systems, and protected and/or sensitive data was not always encrypted. AS personnel with access to critical systems and/or protected data were not always required to complete information security awareness training or sign data confidentiality forms, and AS did not perform a periodic, documented management review of user access privileges within all critical systems and applications containing protected data. In addition, AS did not formally document the evaluation/testing of the quality and security of web applications prior to moving them into the production environment; and daily and weekly backups for AS systems with protected data were not encrypted when stored locally at the AS or campus data centers, or when in-transit to and stored at the off-site storage facility operated by a third-party vendor. Further, AS lacked a comprehensive IT disaster recovery plan for all AS systems, which is a repeat finding from the prior Auxiliary Organizations audit; and the AS Bookstore lacked antivirus software on an application server and workstations used by Bookstore personnel.

INTRODUCTION

BACKGROUND

Education Code §89900 states, in part, that the operation of auxiliary organizations shall be conducted in conformity with regulations established by the Trustees.

Education Code §89904 states, in part, that the Trustees of the California State University (CSU) and the governing boards of the various auxiliary organizations shall:

- ▶ Institute a standard systemwide accounting and reporting system for businesslike management of the operation of such auxiliary organizations.
- ▶ Implement financial standards that will assure the fiscal viability of such various auxiliary organizations. Such standards shall include proper provision for professional management, adequate working capital, adequate reserve funds for current operations and capital replacements, and adequate provisions for new business requirements.
- ▶ Institute procedures to assure that transactions of the auxiliary organizations are within the educational mission of the state colleges.
- ▶ Develop policies for the appropriation of funds derived from indirect cost payments.

The Board of Trustee policy concerning auxiliary organizations was originally adopted in July 1981 in the Resolution of the Committee on Finance (RFIN) 7-81-4. Executive Order 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, represents policy of the Trustees addressing CSU auxiliary organization activity and governing the internal management of the system. CSU auxiliary organizations are required to comply with Board of Trustee policy (California Code of Regulations, Title 5, Section 42402 and Education Code, Section 89900).

This executive order requires that the Office of the University Auditor will perform an internal compliance/internal control review of auxiliary organizations. The review will be used to determine compliance with law, including statutes in the Education Code and rules and regulations of Title 5, and compliance with policy of the Board of Trustees and of the campus, including appropriate separation of duties, safeguarding of assets, and reliability and integrity of information. According to Board of Trustee instruction, each auxiliary organization shall be examined on a triennial basis pursuant to procedures established by the chancellor.

The University Foundation California State University, Chico (University Foundation) was established in 1940 as a non-profit public benefit corporation to support California State University, Chico (CSUC) projects and programs for which state funding is insufficient or not available. In 1997, the University Foundation became solely philanthropic and as such administers the university's gift programs including bequests, charitable trusts, special gifts, charitable gift annuities, scholarships, endowments, and donor-advised funds. The University Foundation is governed by a board of governors comprised of community members, university administrators, a faculty member and a student representative. The University

Foundation does not have employees and relies on The CSU, Chico Research Foundation for gift administration services and the Associated Students of California State University, Chico for accounting and administrative support services.

The CSU, Chico Research Foundation (Research Foundation) was established in 1996 as a non-profit public benefit corporation following a reorganization of the responsibilities of the University Foundation. The Research Foundation assumed responsibility for post-award administration of sponsored programs as well as entrepreneurial activities, including a local radio station, the University Farm, and rental properties. It also acts as a fiscal agent for numerous campus programs and offers expertise and resources to communities in the university's regional service area by enabling such programs as the Center for Economic Development, the Geographical Information Center, the Satellite Education Network, and an adult resources center. The Research Foundation is governed by a board of directors comprised of campus administration, faculty, a student, and members of the community. The Research Foundation relies on Associated Students of California State University, Chico for accounting and administrative support services.

Associated Students of California State University, Chico (AS) was established in 1942 as a non-profit public benefit corporation to provide for student self-government; to provide essential activities closely related to but not normally included as a part of CSUC regular instructional programs; and to promote the educational effectiveness, academic excellence and general welfare of the campus. AS is a comprehensive campus auxiliary serving thousands of students, faculty, staff and community members and is a unique auxiliary in the CSU system because it operates business enterprises (the bookstore and dining services), as well as the student union, recreation center and aquatic center; an early childhood teaching/learning laboratory; a community legal information center; and student government. AS is governed by a board of directors comprised of campus administration, faculty, and student representatives. AS also provides accounting and administrative support services to both the University Foundation and the Research Foundation.

PURPOSE

The principal audit objectives were to determine compliance with the Education Code, Title 5, and directives of the Board of Trustees and the Office of the Chancellor and to assess the adequacy of controls and systems. Specifically, we sought assurances that:

- ▶ Legal and regulatory requirements are complied with.
- ▶ Accounting data is provided in an accurate, timely, complete, or otherwise reliable manner.
- ▶ Assets are adequately safeguarded from loss, damage, or misappropriation.
- ▶ Duties are appropriately segregated consistent with appropriate control objectives.
- ▶ Transactions, accounting entries, or systems output is reviewed and approved.
- ▶ Management does not intentionally override internal controls to the detriment of control objectives.
- ▶ Accounting and fiscal tasks, such as reconciliations, are prepared properly and completed timely.
- ▶ Deficiencies in internal controls previously identified were corrected satisfactorily and timely.
- ▶ Management seeks to prevent or detect erroneous recordkeeping, inappropriate accounting, fraudulent financial reporting, financial loss, and exposure.

SCOPE AND METHODOLOGY

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 accounting and administrative controls are in place and operative. The management review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor policies, letters, and directives. For those audit tests that required annualized data, fiscal years 2007/08 and 2008/09 were the primary periods reviewed. In certain instances, we were concerned with representations of the most current data; in such cases, the test period was July 1, 2009, to December 18, 2009. Our primary focus was on internal compliance/internal control.

Specifically, we reviewed and tested:

- ▶ Formation of the auxiliary.
- ▶ Functions the auxiliary performs on the campus.
- ▶ Creation and operation of the auxiliary's board.
- ▶ Establishment of policies and procedures based upon sound business practices.
- ▶ Maintenance of "arms-length" in business transactions between the auxiliary and the campus.
- ▶ Campus oversight of auxiliary operations.

Additionally, for the period reviewed, we examined other aspects of compliance of the campus and each auxiliary with the Education Code and Title 5 as they relate to the operation of CSU auxiliary organizations. Individual codes and regulations added to the scope of our review were identified through an assessment of risk. Similarly, internal controls were included within our scope based upon risk. Therefore, the scope of our review varied from auxiliary to auxiliary.

A preliminary survey of CSU auxiliaries at each campus was used to identify risks. Risk was defined as the probability that an event or action would adversely affect the auxiliary and/or the campus. Our assessment of risk was based upon a systematic process, using professional judgments on probable adverse conditions and/or events that became the basis for development of our final scope. We sought to assign higher review priorities to activities with higher risks. As a result, not all risks identified were included within the scope of our review.

Based upon this assessment of risks, we specifically included within the scope of our review the following:

The University Foundation California State University, Chico

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance

The University Foundation California State University, Chico (cont.)

- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Cash Receipts and Handling
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Trusts and Other Liabilities
- ▶ Endowment Administration
- ▶ Information Technology

The CSU, Chico Research Foundation

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Auxiliary Programs

Associated Students of California State University, Chico

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll

Associated Students of California State University, Chico (cont.)

- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Auxiliary Programs
- ▶ Information Technology

Campus

- ▶ Campus Oversight and Control

We have not performed any auditing procedures beyond December 18, 2009. Accordingly, our comments are based on our knowledge as of that date. Since the purpose of our comments is to suggest areas for improvement, comments on favorable matters are not addressed.

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

CAMPUS

INFORMATION TECHNOLOGY

The campus did not ensure that the auxiliaries had fully addressed Payment Card Industry (PCI) Data Security Standard (DSS) requirements. This is a repeat finding from our Information Security audit conducted in August 2008.

Although some assessment of PCI DSS compliance for the auxiliaries had been conducted, we found that:

- ▶ Roles and responsibilities for PCI DSS compliance were not adequately defined between the campus and auxiliaries.
- ▶ A compliance risk assessment was not fully completed and documented to determine comprehensive compliance obligations for credit card data maintained on auxiliary servers, transmitted throughout the campus network, and stored manually in local files.
- ▶ An annual PCI DSS Self Assessment Questionnaire (SAQ) was not completed by any of the auxiliaries as is required by PCI DSS of all level one, two and three vendors, and recommended for all level four vendors.

The California State University, Chico (CSUC) *Credit Card Handling Security Standards* state that the campus and all departments that process credit or debit card information must comply with the PCI DSS. This includes the acquiring, accepting, capturing, storing, processing, or transmitting of credit or debit card data, in both electronic and non-electronic formats. Therefore, all campus credit card merchants, including merchants transmitting via a terminal on a dedicated phone line, or other approved method of transmission must complete an annual self-assessment survey and, if applicable, an internal scan and a remote external scan by a PCI DSS approved vendor.

Executive Order (EO) 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

The PCI DSS is a set of comprehensive requirements for enhancing payment account data security, which was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively

protect customer account data. According to payment brand rules, all merchants and their service providers are required to comply with the PCI DSS in its entirety.

The PCI DSS SAQ is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. The PCI DSS SAQ consists of the following two components: (1) Questions correlating to the PCI DSS requirements, appropriate to service providers and merchants; and (2) An attestation of compliance which attests to an organization's certification of eligibility to perform and have performed the appropriate self-assessment.

The campus information security officer stated that the campus and auxiliaries were aware of PCI DSS requirements and had made some progress towards PCI DSS compliance, but had not fully addressed the collective union of campus and auxiliary roles and responsibilities for PCI DSS assessment due to time and resource constraints.

Failure to comply with PCI DSS requirements exposes the auxiliaries and campus to potential financial penalties and credit card usage restrictions, which could include termination of the entities' ability to accept credit cards.

Recommendation 1

We recommend that the campus and auxiliaries that accept credit cards:

- a. Define and document roles, responsibilities, and legal determination for PCI DSS compliance between the campus and the auxiliaries.
- b. Conduct and fully document a risk assessment of comprehensive compliance obligations for credit card data maintained on auxiliary servers and transmitted throughout the campus network and stored manually in local files.
- c. Complete an annual SAQ to include all credit card merchants on campus, whether completed jointly or separate from the auxiliaries.

Campus Response

We concur with the finding. The campus information security office is responsible for establishing and managing data security standards and procedures for the campus and its auxiliary organizations. This responsibility encompasses facilitating PCI DSS compliance. Current efforts are underway to complete SAQs by each campus entity.

Implementation Date: August 31, 2010

THE UNIVERSITY FOUNDATION CALIFORNIA STATE UNIVERSITY, CHICO

OPERATING AND ADMINISTRATIVE AGREEMENTS

Certain agreements between The University Foundation California State University, Chico (University Foundation) and third-party service providers did not include appropriate indemnification provisions.

We found that the indemnification provisions in the agreements with a property management firm and an investment consultant did not specifically indemnify the California State University (CSU) Trustees, the campus, and the State of California.

The California State University Risk Management Authority (CSURMA) Auxiliary Organization Risk Management Authority (AORMA) *Policy & Procedure L-5* states that it is the policy of the CSURMA AORMA Self-Insured Liability Program that member organizations will protect CSURMA program assets by fully implementing the guidelines found in the Insurance Requirements in the Contracts Manual prepared by CSURMA's program administrator. This means that auxiliary organizations will require third-party contractors and vendors to provide appropriate indemnification, insurance, and documentation of coverage.

EO 849, *California State University Insurance Requirements*, dated February 5, 2003, states that auxiliary organizations shall agree to indemnify, defend, and save harmless the State of California, the Trustees of the CSU, the campus, and the officers, employees, volunteers, and agents of each of them from any and all loss, damage, or liability that may be suffered or incurred by state, caused by, arriving out of, or in any way connected with the operations of the auxiliary.

The CSU, Chico Research Foundation (Research Foundation) finance director stated that the auxiliary had assumed a standard property management agreement for commercial real estate held in a charitable remainder trust. He further stated that failure to include a proper indemnification provision in the investment consultant's agreement was due to oversight.

The absence of appropriate indemnification provisions increases the risk of misunderstanding and miscommunication regarding rights and responsibilities and subjects the auxiliary and CSU to potential liability.

Recommendation 2

We recommend that the University Foundation:

- a. Amend the cited agreements with appropriate indemnification provisions.
- b. Ensure that all future agreements include appropriate indemnification provisions.

Campus Response

We concur. Language indemnifying CSUC, the CSU Trustees, and the State of California is currently being added to the cited agreements. In the future, the Research Foundation administration office will coordinate with other campus staff to ensure appropriate indemnification language is included in all University Foundation third-party agreements.

Implementation Date: August 31, 2010

CORPORATE GOVERNANCE

The University Foundation had not filed amended Bylaws with the chancellor's office in a timely manner.

We found amendments to the Bylaws made on April 3, 2007, that had not been filed with the chancellor's office.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* Section 11.6.1, *Reporting Changes in Articles of Incorporation and Bylaws*, states that when an auxiliary organization makes changes to its Articles of Incorporation or Bylaws, a complete amended copy is to be submitted to Financing and Treasury at the Office of the Chancellor within 30 calendar days. The submission should indicate the date the changes were approved by the governing board and/or members.

The Research Foundation finance director stated that the auxiliary was unaware of this requirement.

Failure to file amendments to Bylaws in a timely manner increases the risk of misunderstandings and may increase legal liability.

Recommendation 3

We recommend that the University Foundation file amendments to the Bylaws with the Financing and Treasury department at the Office of the Chancellor within 30 calendar days.

Campus Response

We concur. The amended Bylaws from April 2007 have been filed with the chancellor's office. In the future, a copy of Bylaw changes will be dispatched to the Financing and Treasury department within 30 days.

Implementation Date: Completed

FEES, REVENUES AND RECEIVABLES

University Foundation matching gift procedures did not require that a documented dual review be performed to ensure that funds are administered in accordance with corporate donor requirements.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.3, *Donations, Program Service Fees, Other Income*, states that the auxiliary should establish a written recordkeeping system that enables gifts to be properly received, recorded, and acknowledged in accordance with donor restrictions and other requirements.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates matching gifts undergo a documented dual review process to ensure that funds are appropriately deposited to an eligible recipient in accordance with corporate donor requirements.

The campus interim director of advancement operations stated that the auxiliary was unaware of the requirement to perform dual review of matching gifts.

Insufficient administration of matching gifts increases the likelihood of misdirected funds and campus exposure to liabilities from non-compliance with corporate donor policies.

Recommendation 4

We recommend that the University Foundation update its matching gift procedures to require that a documented dual review be performed to ensure that funds are administered in accordance with corporate donor requirements.

Campus Response

We concur. Advancement operations has implemented additional verification documentation on all matching gifts received, which includes a dual review to ensure that funds are administered in accordance with corporate donor requirements.

Implementation Date: Completed

ENDOWMENT ADMINISTRATION

Certain University Foundation endowment files lacked documented donor intent and scholarship guidelines.

We reviewed 20 endowment files and found that in eight instances, documented donor intent and scholarship guidelines were missing.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.3, *Donations, Program Service Fees, Other Income*, states that the auxiliary should establish a written recordkeeping system that enables gifts to be properly received, recorded, and acknowledged in accordance with donor restrictions and other requirements.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates sufficient administration of endowments.

The campus director of major gifts and planned giving stated that previous auxiliary management sent those documents for storage in a warehouse, and he was unable to retrieve the documents from storage for review by the auditor.

Insufficient administration of endowments increases the risk that errors and irregularities will occur.

Recommendation 5

We recommend that the University Foundation ensure that each endowment file contains documented donor intent and scholarship guidelines.

Campus Response

We concur. New procedures and forms were adopted more than eight years ago to ensure that new endowment files contain documented donor intent and scholarship guidelines signed by the donors. The scholarship advancement coordinator is in the process of systematically reviewing files for endowments established prior to the new procedures to ensure their information is complete.

Implementation Date: April 30, 2011

INFORMATION TECHNOLOGY

INFORMATION SECURITY TRAINING

University Foundation and advancement personnel with access to critical systems or protected data were not required to complete information security awareness training.

The CSUC *Information Security Plan* states that, when appropriate, information security training is provided to individuals whose job functions require specialized skill or knowledge in information

security. While the heads of relevant offices are ultimately responsible for ensuring compliance with information security practices, the information security office will assist in the development of training and education programs for all employees who have access to confidential data. Federal, state, and university policies concerning confidential information should be provided for review before access to protected/confidential information is allowed. The information security program provides and coordinates training for individuals whose job functions require special knowledge of security threats, vulnerabilities, and safeguards. This training is focused on expanding knowledge, skills, and abilities for technical individuals responsible for securing systems and information.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates periodic information security awareness training for all employees with access to protected data.

The campus interim director of advancement operations stated that information security awareness training was provided to some management employees, but management was unaware that such training was required of all employees.

Failure to provide employees with information security awareness training increases the risk of mismanagement of protected data, which increases auxiliary and campus exposure to security breaches and could compromise compliance with statutory information security requirements.

Recommendation 6

We recommend that the University Foundation develop and implement an action plan for providing information security awareness training to all employees with access to critical systems or protected data.

Campus Response

We concur. Advancement operations is currently working with the CSUC security office to provide an information security awareness seminar or an online training module. Completion of training will be required to retain access privileges to the Banner advancement database and the university advancement portal. In addition, this training will be required for all new staff prior to gaining access to the database or portal. Access privileges are reviewed and renewed annually at the beginning of the fiscal year.

Implementation Date: August 31, 2010

DATA SECURITY

Protected data stored in the Banner donor system was not encrypted at the University Foundation.

The CSUC *Server Security Baseline Standards* state that servers storing any protected level-one data should use encryption for both the live production information and for backups of that information.

The CSUC *Data Classification and Protection Standards* state that electronic storage of protected level-one data requires access controls and file protection mechanisms. If these are not found in the operating system in use, then additional security packages are required.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates encryption of any protected data residing on auxiliary systems.

The campus interim director of advancement operations stated that the current version of the Banner application was not delivered with any database encryption, and it was understood that the vendor does not support any form of encryption in this version of the application. She added that it might be possible to employ Oracle's transparent data encryption, but testing of this option had not been performed due to reluctance to make changes to the delivered application that might make the application of updates or upgrades more difficult.

Failure to encrypt protected and/or sensitive donor data could require the auxiliary to notify all affected parties in the event of a breach of security and potentially damage the auxiliary's reputation.

Recommendation 7

We recommend that the University Foundation apply encryption controls to all University Foundation applications, databases, and file servers that house protected and/or sensitive donor data.

Campus Response

We concur. Advancement operations has applied encryption to all Social Security number and credit card fields in the Banner advancement and Campus Call databases.

Implementation Date: Completed

THE CSU, CHICO RESEARCH FOUNDATION

PROPERTY AND EQUIPMENT

Dispositions and acquisitions of CSU, Chico Research Foundation (Research Foundation) property and equipment were only communicated to the Research Foundation once annually by campus property management operations, and thus were not processed in a timely manner.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.7, *Property and Equipment*, states that the auxiliary should establish a written system that ensures proper recording of property and equipment when received and for labeling of equipment.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates sufficient administration of property and equipment.

The Research Foundation finance director stated that the Research Foundation operated under a policy that only required annual reporting and was unaware of the need to report dispositions more frequently.

Insufficient administration of property and equipment increases the risk of misstated property records and theft, loss, or unauthorized use of auxiliary property.

Recommendation 8

We recommend that the Research Foundation require campus property management operations to communicate dispositions/acquisitions of property and equipment on a quarterly basis.

Campus Response

We concur. The Research Foundation agrees that the campus property management office should be required to communicate dispositions/acquisitions of property and equipment on a quarterly basis. Procedures for property reconciliation, including quarterly communications, will be updated and implemented.

Implementation Date: September 30, 2010

TRUSTS AND OTHER LIABILITIES

The Research Foundation had not completed a review of its custodial trust accounts to determine the source of deposits, and therefore, certain campus program revenues may be inappropriately deposited to, and held in custody by, the Research Foundation.

The Research Foundation financial statements as of June 30, 2009, indicated that the Research Foundation administered and maintained 564 custodial trust accounts totaling \$6,392,711. We reviewed 66 of these accounts for which trust account agreements were available and found that state/campus operating funds may be inappropriately held by the Research Foundation in nearly all of the accounts.

EO 919, *Policy Governing Non-General Fund Receipts*, dated October 15, 2004, states that each CSU campus shall administer their non-General Fund receipts to ensure that the funds are held in proper accounts. EO 919 also states that, as a matter of CSU policy, auxiliaries may not accept state funds with the intent of administering them as an agent of the university. Payment for services is the only instance where state funds may be accepted into an auxiliary organization's account. Further, the entity that is responsible for any losses that might arise from the event or activity that generated the receipts shall be the entity wherein receipts are held.

Although EO 1000, *Delegation of Fiscal Authority and Responsibility*, dated July 1, 2007, indicates that it supersedes EO 919, the areas noted above are acknowledged by systemwide administrators to still be in effect and will be addressed by the forthcoming Integrated CSU Administrative Manual.

The Research Foundation finance director stated that the custodial trust accounts are renewed every three years and the renewal process requires the review of source(s) of funds that are deposited into a campus program account held in custody by the Research Foundation. He further stated that the Research Foundation relies on the information provided on the authorization form and does not subsequently review every deposit upon receipt to determine if the source of funds is consistent with the information provided on the approved form.

The campus' required oversight of state/campus operating funds is limited when funds are deposited outside the custody of the chief financial officer.

Recommendation 9

We recommend that the Research Foundation:

- a. Complete a review of all custodial trust accounts and determine, within 60 days, which accounts contain state/campus operating funds.
- b. Certify that none of the following specific and similar monies reside in Research Foundation accounts:
 - Contracts and grants awarded to the university.

- Research Foundation net operating surplus designated for use by the campus.
 - Fees for continuing education courses provided by the university.
 - Fees for university events, workshops, conferences, institutes, special projects, and programs.
 - Athletics funds/fees/revenues other than gifts/donations.
 - Investment income from state funds/fees/revenues.
 - Reimbursements for services and products provided to auxiliary enterprises and organizations paid from General Fund and/or CSU operating fund monies.
 - Rental fees for university facilities, except those facilities that have been leased to the auxiliary by the campus.
 - Student fees and other general fees pursuant to the CSU student fee policy.
 - Monies held by the Research Foundation via contract with the campus.
- c. Submit to the Office of the University Auditor, within 60 days, a list of those trust accounts which have been deemed appropriate to remain in the custody of the Research Foundation and comprehensive documentation to support the sources of funds for those trust accounts.
- d. Move those state funds identified in “a” above to campus accounts within six months.

Campus Response

While we concur with the above recommendations, resource constraints make the proposed dates unattainable using campus staff. However, with the help of the Office of the University Auditor, a review of the accounts will commence on August 2, 2010. Upon completion of that review, we will develop and implement a plan to transfer programs/funds to the campus, as appropriate.

ASSOCIATED STUDENTS OF CALIFORNIA STATE UNIVERSITY, CHICO

FISCAL COMPLIANCE

Unrelated business income (UBI) for servicing and repairing of Apple computer equipment provided to the public (non-students) was not accounted for/reported by Associated Students of California State University, Chico (AS).

Internal Revenue Code §512 through §514 defines an unrelated trade or business of an exempt organization as any trade of business, the conduct of which is not substantially related to the exercise or performance of its tax-exempt purpose. UBI in excess of \$1,000 must be reported to the Internal Revenue Service (IRS), whether or not a tax liability is incurred. In addition, the organization's tax-exempt status may be jeopardized if too large a portion of its revenue is derived from UBI.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates the establishment of a system to track and account for UBI.

The AS associate financial services director stated that due to an oversight, the income associated with servicing Apple computers had not been reported as UBI for income tax reporting purposes

Failure to properly analyze, document, and report UBI increases the auxiliary's exposure to potential penalties and actions by the IRS.

Recommendation 10

We recommend that AS account for and track UBI for servicing and repairing of Apple computer equipment provided to the public, and file federal income tax returns as appropriate.

Campus Response

We concur with the recommendation. Procedures will be put in place for tracking and reporting Apple computer service UBI received from the public. This income will be included in the federal income tax returns, as appropriate.

Implementation Date: December 31, 2010

CASH RECEIPTS AND HANDLING

Accountability for cash receipts at the AS Butte and Holt convenience store locations required improvement.

We found that:

- ▶ Separate logons and closeout procedures were not used to establish accountability when multiple cashiers used the same cash register.
- ▶ Accountability for daily cash collections was not determined prior to transport to the AS business office, as cashiers did not conduct cash counts at the end their shifts.
- ▶ Daily closeout procedures did not include reconciliation of cash collected and sales register totals.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.1, *Cash*, states that the auxiliary should receive cash in a consistent manner utilizing systems that ensure integrity of existing internal controls.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates the accountability for cash or negotiable instruments to a specific employee from the time of receipt to deposit.

The AS director of dining services stated that due to the limited safe size at these locations, it has not been feasible to have separate cash drawers for each cashier. She added that due to the limited amount of secure space, it has not been feasible to perform closeout procedures at the convenience store locations.

Inadequate control over cash receipts increases exposure to loss from inappropriate acts.

Recommendation 11

We recommend that AS:

- a. Localize accountability over cash receipts when multiple cashiers operate the same cash register.
- b. Require cashiers to conduct cash counts at the end of their shifts, and supervisors to conduct secondary cash counts to confirm the accuracy of cashier counts.
- c. Reconcile cash collected to daily sales totals as part of the closeout procedures.

Campus Response

We concur with the recommendation. Procedures are in place at Butte and Holt stations to localize accountability over cash receipts when multiple cashiers operate the same cash register in some locations. Cashiers will conduct cash counts at the end of their shifts at all locations and supervisors will confirm the accuracy of cashier counts. Cash collected will be reconciled with the daily sale total as part of the closeout procedure.

Implementation Date: July 31, 2010

PERSONNEL AND PAYROLL

The AS payroll system did not generate a report of pay rate changes for management review.

We reviewed payroll system reports for four payroll cycles and found that in all cycles reviewed, the payroll system did not generate a pay rate edit listing report for pay rate changes since the prior payroll cycle for management review. Such a report and management review would ensure that there were no undetected errors or unauthorized changes to employee salary and wage rates.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.6, *Payroll*, states that the auxiliary should establish a written system that ensures accurate and timely collection of payroll information such as changes in salary and wage rate.

The AS associate financial services director stated that all employee pay rate changes are supported by an approved personnel action form. She also stated that payroll changes are reviewed but are done so informally without the use of a payroll edit listing report.

The absence of a payroll system report to monitor pay rate changes that is reviewed by management increases the risk of inappropriate modifications to salary and wage rates.

Recommendation 12

We recommend that AS modify its payroll system to generate a pay rate edit listing report for each payroll cycle and require appropriate management review.

Campus Response

We concur with the recommendation. A payroll system report will be created that tracks employee pay rate changes entered since the prior payroll cycle. The report will be reviewed by management prior to distributing each subsequent payroll.

Implementation Date: December 31, 2010

INFORMATION TECHNOLOGY

PASSWORD SECURITY

Password and login security controls were not always adequate for AS systems.

We found that:

- ▶ The password and login security parameters for the Integrated Financial and Accounting System (IFAS) accounting system did not enforce any minimum password length, password complexity, periodic expiration, or login security. Instead, the information technology (IT) administrator set the passwords for users at eight characters, with a combination of numbers and letters.
- ▶ The password and login security parameters for the CDD.net system, a web-based IFAS financial reporting tool, did not enforce any minimum password length, password complexity, periodic expiration, or login security, and used the same user names and passwords as set in IFAS.
- ▶ The password and login security parameters for the TimeCentre time, attendance, and payroll system did not enforce any minimum password length, password complexity, periodic expiration, or login security.

The CSUC *Password Policy*, dated November 8, 2007, requires that passwords be 8-32 characters in length; contain at least one lowercase letter, at least one uppercase letter, at least one number, and at least one symbol (e.g. ~!@#\$%^*?); not contain an user ID, a dictionary word longer than 8 characters, and repetitive or sequential characters (e.g., aaaa, 1234); and not have been previously used.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates strong password and login parameters.

The AS IT director stated that there is no mechanism available on either the IFAS or CDD.Net systems to enforce password standards or allow a user to change their password to meet such standards. He further stated that there is no mechanism within the TimeCentre system to enforce password standards.

Insufficient password and login parameters may compromise the authentication credentials of user account privileges that are embedded into applications and operating systems, which increase the risk of unauthorized access to auxiliary systems and confidential data.

Recommendation 13

We recommend that AS set effective password and login security parameters for the IFAS, CDD.net and TimeCentre systems in accordance with campus password standards and leading security industry guidelines, and also perform an assessment of password security parameters for all other AS systems.

Campus Response

We concur with this finding. A more stringent password requirement will be implemented in IFAS and CDD.Net. The TimeCentre system does not have the capability to age passwords or set criteria on how complex passwords have to be. A new timekeeping system has been budgeted for fiscal year 2010/11 and will be implemented to address the finding,

Implementation Date for IFAS and CDD.net: December 31, 2010

Implementation Date for TimeCentre: June 30, 2011

DATA SECURITY

Protected and/or sensitive data was not always encrypted at AS.

We found that:

- ▶ Protected data stored in the IFAS accounting system was not encrypted.
- ▶ The AS file server utilized by all AS employees employed no encryption controls and was noted on the AS System Profiles/Risk Assessment to contain a wide variety of data, including financial transactions, salary and payroll information, social security numbers (possibly), tax information (including employee tax data), employee personal information (phone numbers, addresses, beneficiaries, etc.), human resources actions, and email archives.

The CSUC *Server Security Baseline Standards* state that servers storing any protected level-one data should use encryption for both the live production information and for backups of that information.

The CSUC *Data Classification and Protection Standards* state that electronic storage of protected level-one data requires access controls and file protection mechanisms. If these are not found in the operating system in use, then additional security packages are required.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that

allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates encryption of any protected data residing on auxiliary systems.

The AS IT director stated that the IFAS system does not have the capability of encrypting protected data at the field level. He further stated that there are no well-established best practices for using file-system based encryption on Windows servers, and the campus information security office has not developed a policy on encryption of such systems.

Failure to encrypt protected and/or sensitive data could require the auxiliary to notify all affected parties in the event of a breach of security and potentially damage the auxiliary's reputation.

Recommendation 14

We recommend that AS apply encryption controls to all AS applications, databases, and file servers that contain protected and/or sensitive data.

Campus Response

We concur with this finding for the IFAS accounting system. However, the current version of IFAS does not support field-level encryption. The university accepts the risk of not having data encryption of protected data in IFAS. In 2011, we will begin evaluating financial systems to replace the version of IFAS currently in use. One requirement of the replacement system will be to have the capability of encrypting confidential data. The AS expects to complete this transition by June 2012.

We concur with the finding for the AS file server. The AS will work with the university information security office and network operations to develop a comprehensive approach to data encryption on AS file servers.

Implementation Date for IFAS: November 30, 2011

Implementation Date for AS file server: June 30, 2011

INFORMATION SECURITY TRAINING AND DATA CONFIDENTIALITY FORMS

AS personnel with access to critical systems and/or protected data were not always required to complete information security awareness training or sign data confidentiality forms.

The CSUC *Information Security Plan* states that, when appropriate, information security training is provided to individuals whose job functions require specialized skill or knowledge in information security. While the heads of relevant offices are ultimately responsible for ensuring compliance with information security practices, the information security office will assist in the development of training and education programs for all employees who have access to confidential data. Federal, state, and university policies concerning confidential information should be provided for review before access to protected/confidential information is allowed. The information security program provides and coordinates training for individuals whose job functions require special knowledge of

security threats, vulnerabilities, and safeguards. This training is focused on expanding knowledge, skills, and abilities for technical individuals responsible for securing systems and information.

The CSUC *Data Classification and Protection Standards* state that an employee must have signed a confidentiality statement before access is granted to systems containing protected level-one data.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates periodic information security awareness training and signed data confidentiality forms for all employees with access to protected data.

The AS IT director stated that the campus information security office, who sets IT security standards for CSUC and its auxiliaries, had not established a policy requiring users of protected data to sign confidentiality agreements or take security awareness training until this past year; and AS had not yet complied with that requirement because of the policy's recent adoption.

Failure to provide employees with information security awareness training increases the risk of mismanagement of protected data, while the lack of signed data confidentiality forms increases the risk of inappropriate disclosure of data and auxiliary exposure to liability for any such disclosures.

Recommendation 15

We recommend that AS:

- a. Develop and implement an action plan for providing information security awareness training to all employees with access to critical systems or protected data.
- b. Establish a policy requiring signed data confidentiality forms from all employees prior to granting them access to critical systems and protected data.
- c. Obtain completed data confidentiality forms from personnel who currently have access to such data.

Campus Response

We concur with this finding. The AS will require users that access systems with protected data to sign data confidentiality agreements and require that these users receive information security training.

Implementation Date: December 31, 2010

USER ACCESS REVIEWS

AS did not perform a periodic, documented management review of user access privileges within all critical systems and applications containing protected data, but instead only completed an annual review of user access to the payroll and human resources applications within the IFAS accounting system.

The CSUC *Account Management Standards* state that all accounts shall be reviewed at least annually to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. This review must be documented. The information security office may also conduct periodic reviews for any system connected to the CSUC network.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.10, *Computer Controls*, states that auxiliary organizations should establish written policies and practices creating levels of security linked to job responsibilities and data sensitivity.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates a periodic, documented review of user access privileges within all systems and applications containing protected data.

The AS IT director stated that while reviews have been done of all systems, they were not documented because the requirement was unknown.

Failure to periodically perform a documented review of user access to critical systems and applications containing protected data increases the risk of inappropriate access, compromised production systems, and potential disclosure of confidential data.

Recommendation 16

We recommend that AS conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually.

Campus Response

We concur with this finding and will implement quarterly reviews of user access privileges within AS systems that contain protected data.

Implementation Date: December 31, 2010

WEB APPLICATION SECURITY

AS did not formally document the evaluation/testing of the quality and security of web applications prior to moving them into the production environment.

The CSUC *Application Code Development Standards* state that the application testing process is vital in identifying security flaws before the application is released. Developers need to test the application's security controls to verify they are working properly, prior to deploying the system into a production environment. Test plans and test results should be documented.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates documented evaluation/testing of the quality and security of web applications prior to moving them into the production environment.

The AS IT director stated that while programs are developed using best security practices, evaluation and testing have not been formally documented because the requirement was unknown.

Failure to formally document evaluation and testing of the quality and security of web applications increases the risk that website applications may contain vulnerabilities that could lead to a loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

Recommendation 17

We recommend that AS perform documented evaluation/testing of the quality and security of web applications prior to moving them into the production environment.

Campus Response

We concur with the finding. Formal documentation of evaluation and testing will be undertaken with any future systems that are developed in-house.

Implementation Date: December 31, 2010

SYSTEM BACKUPS

Daily and weekly backups for AS systems with protected data were not encrypted when stored locally at the AS or campus data centers, or when in-transit to and stored at the off-site storage facility operated by a third-party vendor.

The CSUC *Server Security Baseline Standards* state that servers storing any protected level-one data should use encryption for both the live production information and for backups of that information.

The CSUC *Data Classification and Protection Standards* state that backups must be encrypted when containing protected level-one data.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates the encryption of protected data contained on auxiliary systems and backups.

The AS IT director stated that the backup systems currently used by the AS do not include the capability of encrypting data.

Inadequate security of system backups increases the risk of inappropriate access to protected data and the possible ramifications of required public notifications should backups be lost when unencrypted.

Recommendation 18

We recommend that AS encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure.

Campus Response

We concur with this finding. The application currently used for backing up data does not support encryption. The IT department is evaluating backup and archiving systems to replace the current application and will implement a new system.

Implementation Date: December 31, 2010

DISASTER RECOVERY PLAN

AS lacked a comprehensive IT disaster recovery plan (DRP) for all AS systems. This is a repeat finding from the prior Auxiliary Organizations audit.

We found that a DRP specifically for the IFAS accounting system was in draft form, but it did not address all critical AS systems including the Micros Cashiering and the Missouri Book System (MBS).

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.10, *Computer Controls*, states that auxiliary organizations should establish written policies and practices that ensure secure computer system operations, including backup and recovery mechanisms and disaster recovery programs.

The AS IT director stated that a comprehensive IT DRP for all AS systems managed by the IT department is currently being developed, but was not yet complete due to other priorities.

The absence of a comprehensive IT DRP increases the risk that business and data processing operations may not be restored within a reasonable time frame in the event of an emergency or disaster.

Recommendation 19

We recommend that AS complete a comprehensive IT DRP, which is inclusive of all critical systems.

Campus Response

We concur with this finding. Backup of data, which is typically part of a DRP, is addressed in the response to the System Backups finding. We intend to draft and adopt a DRP for critical AS systems before the end of the year.

Implementation Date: December 31, 2010

ANTIVIRUS SOFTWARE

The AS Bookstore lacked antivirus software on the AS 400 MBS application server and Mac workstations used by Bookstore personnel.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that antivirus software be employed on all critical systems.

The AS Bookstore operations/information security manager stated that the Bookstore had not considered the need for antivirus software for the MBS server and Mac workstations.

The lack of antivirus software on critical servers and user workstations increases the risk that machines become infected with computer viruses that could lead to a loss of protected confidential information and/or the execution of malicious programs that could disable additional network resources.

Recommendation 20

We recommend that AS employ antivirus software on the AS 400 MBS application server and Mac workstations, as well as on all other Bookstore systems.

Campus Response

We concur with the recommendation regarding antivirus software for the Mac workstations. Procedures will be developed to ensure all existing and new workstations have antivirus software. We are researching with our system provider regarding employing antivirus software on the AS 400 MBS.

Implementation Date: December 31, 2010

APPENDIX A: PERSONNEL CONTACTED

Name

Title

CAMPUS

Paul J. Zingg	President
Robert Alber	Senior Associate Vice President, University Advancement
Teresa Arnold	Executive Assistant to the Vice President for Business and Finance
Brooke Banks	Information Security Officer
Richard Ellison	Vice President, University Advancement
Robyn Hafer	Interim Director of Advancement Operations, University Advancement
Lorraine Hoffman	Vice President for Business and Finance
Mark McGee	Programmer/Analyst, University Advancement
Jeremy Pollard	Programmer/Analyst, University Advancement
Gary Salberg	Director of Major Gifts/Planned Giving, University Advancement

THE UNIVERSITY FOUNDATION CALIFORNIA STATE UNIVERSITY, CHICO

Richard Ellison	Secretary
Lorraine Hoffman	Treasurer

THE CSU, CHICO RESEARCH FOUNDATION

Michele Flowerdew	Senior Analyst
Richard Jackson	Executive Director
Carol Sager	Director, Office of Research and Sponsored Programs
Fred Woodmansee	Finance Director

ASSOCIATED STUDENTS OF CALIFORNIA STATE UNIVERSITY, CHICO

David Buckley	Executive Director
Brian Buie	Programmer Analyst
Darlene Chester	Convenience Store Supervisor
Peggy Devol	Accounts Payable Supervisor
Steve Dubey	Bookstore Director
Joyce Friedman	Financial Services Director
Cindy Haws	Dining Service Accounting Assistant
Corinne Hileman	Retail Dining Manager
Marilyn Hoag	Bookstore Operations/Information Security Manager
Susan Jennings	Associate Financial Services Director
Yves LaTouche	Dining Services Director
Nancy Mantle	Bookstore Associate Director
Matt Norby	Information Technology Director
Gwen Preszler	Clothing Buyer
Linda Riggins	Textbook Department Supervisor
Chuck Samuels	Supply Buyer
Rick Scott	Recreation Center Director
Jeffery Soon	Associate Dining Services Director

STATEMENT OF INTERNAL CONTROLS

A. INTRODUCTION

Internal accounting and related operational controls established by the State of California, the California State University Board of Trustees, and the Office of the Chancellor are evaluated by the University Auditor, in compliance with professional standards for the conduct of internal audits, to determine if an adequate system of internal control exists and is effective for the purposes intended. Any deficiencies observed are brought to the attention of appropriate management for corrective action.

B. INTERNAL CONTROL DEFINITION

Internal control, in the broad sense, includes controls that may be characterized as either accounting or operational as follows:

1. Internal Accounting Controls

Internal accounting controls comprise the plan of organization and all methods and procedures that are concerned mainly with, and relate directly to, the safeguarding of assets and the reliability of financial records. They generally include such controls as the systems of authorization and approval, separation of duties concerned with recordkeeping and accounting reports from those concerned with operations or asset custody, physical controls over assets, and personnel of a quality commensurate with responsibilities.

2. Operational Controls

Operational controls comprise the plan of organization and all methods and procedures that are concerned mainly with operational efficiency and adherence to managerial policies and usually relate only indirectly to the financial records.

C. INTERNAL CONTROL OBJECTIVES

The objective of internal accounting and related operational control is to provide reasonable, but not absolute, assurance as to the safeguarding of assets against loss from unauthorized use or disposition, and the reliability of financial records for preparing financial statements and maintaining accountability for assets. The concept of reasonable assurance recognizes that the cost of a system of internal accounting and operational control should not exceed the benefits derived and also recognizes that the evaluation of these factors necessarily requires estimates and judgment by management.

D. INTERNAL CONTROL SYSTEMS LIMITATIONS

There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal accounting and related operational control. In the performance of most control procedures, errors can result from misunderstanding of instruction, mistakes of judgment, carelessness, or other personal factors. Control procedures whose effectiveness depends upon segregation of duties can be circumvented by collusion. Similarly, control procedures can be circumvented intentionally by management with respect to the executing and recording of transactions. Moreover, projection of any evaluation of internal accounting and operational control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions and that the degree of compliance with the procedures may deteriorate. It is with these understandings that internal audit reports are presented to management for review and use.

California State University, Chico
 Chico, California 95929-0150
 Office of the President
 530-898-5201
 Fax: 530-898-5077



July 6, 2010

RECEIVED
 UNIVERSITY AUDITOR

JUL - 7 2010

THE CALIFORNIA STATE
 UNIVERSITY

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



Subject: Auxiliary Organizations Audit Report 09-19

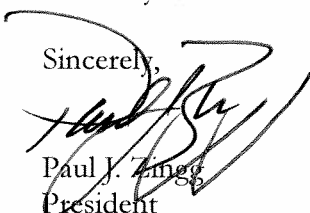
Dear Mr. Mandel:

Enclosed is CSU Chico's response to our Auxiliary Organizations Audit Report 09-19 at California State University, Chico. As instructed by your staff, we have included the recommendations as stated in the audit report, a response for each recommendation and an anticipated implementation date for each response.

Under separate cover are statements of corrective action for some of our findings that have been already been implemented.

If you have any questions, please contact Lori Hoffman by phone at (530) 898-6231 or by email at lbhoffman@csuchico.edu. Thank you.

Sincerely,


 Paul J. Zingg
 President

Enclosure

cc: Lorraine B. Hoffman

AUXILIARY ORGANIZATIONS
CALIFORNIA STATE UNIVERSITY,
CHICO

Audit Report 09-19

CAMPUS

INFORMATION TECHNOLOGY

Recommendation 1

We recommend that the campus and auxiliaries that accept credit cards:

- a. Define and document roles, responsibilities, and legal determination for PCI DSS compliance between the campus and the auxiliaries.
- b. Conduct and fully document a risk assessment of comprehensive compliance obligations for credit card data maintained on auxiliary servers and transmitted throughout the campus network and stored manually in local files.
- c. Complete an annual SAQ to include all credit card merchants on campus, whether completed jointly or separate from the auxiliaries.

Campus Response

THE UNIVERSITY FOUNDATION CALIFORNIA STATE UNIVERSITY, CHICO

OPERATING AND ADMINISTRATIVE AGREEMENTS

Recommendation 2

We recommend that the University Foundation:

- a. Amend the cited agreements with appropriate indemnification provisions.
- b. Ensure that all future agreements include appropriate indemnification provisions.

Campus Response

CORPORATE GOVERNANCE

Recommendation 3

We recommend that the University Foundation file amendments to the Bylaws with the Financing and Treasury department at the Office of the Chancellor within 30 calendar days.

Campus Response

FEES, REVENUES AND RECEIVABLES

Recommendation 4

We recommend that the University Foundation update its matching gift procedures to require that a documented dual review be performed to ensure that funds are administered in accordance with corporate donor requirements.

Campus Response

ENDOWMENT ADMINISTRATION

Recommendation 5

We recommend that the University Foundation ensure that each endowment file contains documented donor intent and scholarship guidelines.

Campus Response

INFORMATION TECHNOLOGY

INFORMATION SECURITY TRAINING

Recommendation 6

We recommend that the University Foundation develop and implement an action plan for providing information security awareness training to all employees with access to critical systems or protected data.

Campus Response

DATA SECURITY

Recommendation 7

We recommend that the University Foundation apply encryption controls to all University Foundation applications, databases, and file servers that house protected and/or sensitive donor data.

Campus Response

THE CSU, CHICO RESEARCH FOUNDATION

PROPERTY AND EQUIPMENT

Recommendation 8

We recommend that the Research Foundation require campus property management operations to communicate dispositions/acquisitions of property and equipment on a quarterly basis.

Campus Response

TRUSTS AND OTHER LIABILITIES

Recommendation 9

We recommend that the Research Foundation:

- a. Complete a review of all custodial trust accounts and determine, within 60 days, which accounts contain state/campus operating funds.
- b. Certify that none of the following specific and similar monies reside in Research Foundation accounts:
 - Contracts and grants awarded to the university.
 - Indirect costs attributable to campus pre-award activities.
 - Research Foundation net operating surplus designated for use by the campus.
 - Fees for continuing education courses provided by the university.
 - Fees for university events, workshops, conferences, institutes, special projects, and programs.
 - Athletics funds/fees/revenues other than gifts/donations.
 - Investment income from state funds/fees/revenues.
 - Reimbursements for services and products provided to auxiliary enterprises and organizations paid from General Fund and/or CSU operating fund monies.
 - Rental fees for university facilities, except those facilities that have been leased to the auxiliary by the campus.
 - Student fees and other general fees pursuant to the CSU student fee policy.
 - Monies held by the Research Foundation via contract with the campus.
- c. Submit to the Office of the University Auditor, within 60 days, a list of those trust accounts which have been deemed appropriate to remain in the custody of the Research Foundation and comprehensive documentation to support the sources of funds for those trust accounts.
- d. Move those state funds identified in “a” above to campus accounts within six months.

Campus Response

ASSOCIATED STUDENTS OF CALIFORNIA STATE UNIVERSITY, CHICO

FISCAL COMPLIANCE

Recommendation 10

We recommend that AS account for and track UBI for servicing and repairing of Apple computer equipment provided to the public, and file federal income tax returns as appropriate.

Campus Response

CASH RECEIPTS AND HANDLING

Recommendation 11

We recommend that AS:

- a. Localize accountability over cash receipts when multiple cashiers operate the same cash register.
- b. Require cashiers to conduct cash counts at the end of their shifts, and supervisors to conduct secondary cash counts to confirm the accuracy of cashier counts.
- c. Reconcile cash collected to daily sales totals as part of the closeout procedures.

Campus Response

PERSONNEL AND PAYROLL

Recommendation 12

We recommend that AS modify its payroll system to generate a pay rate edit listing report for each payroll cycle and require appropriate management review.

Campus Response

INFORMATION TECHNOLOGY

PASSWORD SECURITY

Recommendation 13

We recommend that AS set effective password and login security parameters for the IFAS, CDD.net and TimeCentre systems in accordance with campus password standards and leading security industry guidelines, and also perform an assessment of password security parameters for all other AS systems.

Campus Response

DATA SECURITY

Recommendation 14

We recommend that AS apply encryption controls to all AS applications, databases, and file servers that contain protected and/or sensitive data.

Campus Response

INFORMATION SECURITY TRAINING AND DATA CONFIDENTIALITY FORMS

Recommendation 15

We recommend that AS:

- a. Develop and implement an action plan for providing information security awareness training to all employees with access to critical systems or protected data.
- b. Establish a policy requiring signed data confidentiality forms from all employees prior to granting them access to critical systems and protected data.
- c. Obtain completed data confidentiality forms from personnel who currently have access to such data.

Campus Response

USER ACCESS REVIEWS

Recommendation 16

We recommend that AS conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually.

Campus Response

WEB APPLICATION SECURITY

Recommendation 17

We recommend that AS perform documented evaluation/testing of the quality and security of web applications prior to moving them into the production environment.

Campus Response

SYSTEM BACKUPS

Recommendation 18

We recommend that AS encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure.

Campus Response

DISASTER RECOVERY PLAN

Recommendation 19

We recommend that AS complete a comprehensive IT DRP, which is inclusive of all critical systems.

Campus Response

ANTIVIRUS SOFTWARE

Recommendation 20

We recommend that AS employ antivirus software on the AS 400 MBS application server and Mac workstations, as well as on all other Bookstore systems.

Campus Response

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

CHANNEL ISLANDS

August 30, 2010

CHICO

DOMINGUEZ HILLS

MEMORANDUM

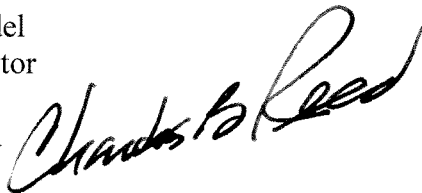
EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FULLERTON

FROM: Charles B. Reed
Chancellor



HUMBOLDT

SUBJECT: Draft Final Report 09-19 on *Auxiliary Organizations*,
California State University, Chico

LONG BEACH

LOS ANGELES

MARITIME ACADEMY

In response to your memorandum of August 30, 2010, I accept the response as submitted with the draft final report on *Auxiliary Organizations*, California State University, Chico.

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/amd

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS