

AUXILIARY ORGANIZATIONS
CALIFORNIA STATE UNIVERSITY,
SACRAMENTO

Audit Report 11-01
July 1, 2011

Members, Committee on Audit

Henry Mendoza, Chair
Melinda Guzman, Vice Chair
Margaret Fortune Steven M. Glazer
William Hauck Hsing Kung Linda Lang

Staff

University Auditor: Larry Mandel
Senior Director: Mike Caldera
Audit Manager: Gary Miller
Senior Auditors: Jamarr Johnson, Caroline Lee,
Dominick Owens, Ken Tsui and Salesian Yuen
Internal Auditor: Kim Tran

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction.....	7
Background	7
Purpose.....	10
Scope and Methodology	10

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

CAMPUS

Fiscal Compliance.....	14
Campus Oversight and Control.....	15
Information Technology	16
Password Security.....	16
Disaster Recovery Plan.....	17

THE UNIVERSITY FOUNDATION AT SACRAMENTO STATE

Operational Compliance	19
Risk Management	19
Conflict of Interest.....	20

UNIVERSITY ENTERPRISES, INC.

Operating and Administrative Agreements	21
Fees, Revenues, and Receivables	22
Auxiliary Programs.....	24
Information Technology	25
Data and Security Assessment.....	25
Network Security	26
Domain Administration	28
System Backups	28
Disaster Recovery Plan.....	29

UNIVERSITY ENTERPRISES DEVELOPMENT GROUP

Facilities Agreements	31
-----------------------------	----

CAPITAL PUBLIC RADIO, INC.

Operating and Administrative Agreements 33

Operational Compliance 35

Fees, Revenues, and Receivables 36

 Accounts Receivable..... 36

 Matching Gifts 37

Information Technology 39

 Payment Card Industry Data Security Standard Compliance 39

 Password and Data Security 41

 User Access Review 43

 Domain Administration 43

 Network Administration 45

 Information Security Awareness Training..... 45

 Disaster Recovery Plan 46

ASSOCIATED STUDENTS OF CALIFORNIA STATE UNIVERSITY, SACRAMENTO

Operational Compliance 48

Segregation of Duties..... 48

Cash Receipts and Handling 49

Fees, Revenues, and Receivables 51

Personnel and Payroll 52

Property and Equipment 52

Information Technology 54

UNIVERSITY UNION OPERATION OF CALIFORNIA STATE UNIVERSITY, SACRAMENTO

Operating and Administrative Agreements 56

Purchasing and Accounts Payable 57

Property and Equipment 57

APPENDICES

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

ABBREVIATIONS

AORMA	Auxiliary Organizations Risk Management Authority
ASI	Associated Students of California State University, Sacramento
CFO	Chief Financial Officer
CIO	Chief Information Officer
CPR	Capital Public Radio, Inc.
CPRE	Capital Public Radio Endowment, Inc.
CSU	California State University
CSURMA	California State University Risk Management Authority
CSUS	California State University, Sacramento
DRP	Disaster Recovery Plan
DSS	Data Security Standard
EO	Executive Order
FY	Fiscal Year
Foundation	The University Foundation at Sacramento State
ICSUAM	Integrated California State University Administrative Manua
IRT	Information Resources and Technology
IT	Information Technology
OMB	Office of Management and Budget
PCI	Payment Card Industry
RFIN	Resolution of the Committee on Finance
T91	Tower 91, Inc.
UEDG	University Enterprises Development Group
UEI	University Enterprises, Inc.
Union	University Union Operation of California State University, Sacramento

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, Sacramento (CSUS) 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 CSUS campus and its auxiliary organizations from January 18, 2011, through February 18, 2011, and made a study and evaluation of the system of internal compliance/internal control in effect as of February 18, 2011. This report represents our triennial review.

Our study and evaluation at *The University Foundation at Sacramento State* 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 February 18, 2011, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *University Enterprises, Inc.* 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 February 18, 2011, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *University Enterprises Development Group* 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 February 18, 2011, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *Capital Public Radio, Inc.* 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 the following areas: fees, revenues and receivables, and 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 February 18, 2011, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *Associated Students of California State University, Sacramento* 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 February 18, 2011, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *University Union Operation of California State University, Sacramento* 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 February 18, 2011, 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

FISCAL COMPLIANCE [14]

The campus had not required full reimbursement by the auxiliaries for indirect costs incurred by the campus for public safety and information resources and technology (IRT) support services provided to the auxiliaries.

CAMPUS OVERSIGHT AND CONTROL [15]

The interrelationship between Capital Public Radio, Inc. (CPR), Capital Public Radio Endowment, Inc., and Tower 91, Inc., may provide unacceptable risk to the campus and the CSU.

INFORMATION TECHNOLOGY [16]

Password controls were not adequate for donor systems administered by the campus, and the campus information technology disaster recovery plan did not include adequate details for the recovery of the donor systems.

THE UNIVERSITY FOUNDATION AT SACRAMENTO STATE

OPERATIONAL COMPLIANCE [19]

The University Foundation at Sacramento State had not developed a comprehensive written risk management policy and had not obtained annual conflict-of-interest statements from all board members.

UNIVERSITY ENTERPRISES, INC.

OPERATING AND ADMINISTRATIVE AGREEMENTS [21]

Certain agreements between University Enterprises, Inc. (UEI) and third parties did not include appropriate provisions for indemnification or the right to audit.

FEES, REVENUES, AND RECEIVABLES [22]

UEI administration of sales revenues audits for the outsourced food and dining services vendors needed improvement, as UEI had not developed written policies and procedures for periodic audits of the outsourced vendors' sales revenues for verification of accurate commissions paid to UEI, and sales audits were not always completed in a timely manner, nor performed by an independent person.

AUXILIARY PROGRAMS [24]

The UEI effort certification process did not consider other campus work assignments for faculty members. This is a repeat finding from the prior Auxiliary Organizations audit.

INFORMATION TECHNOLOGY [25]

Protected and/or sensitive data was not encrypted when stored in the UEI accounting and payroll systems, and UEI did not perform an assessment and inventory of protected data residing on an administrative file server. Also, the UEI network did not place Internet-accessible web servers on a separate network segment from other production servers. In addition, UEI operated an independent Active Directory domain in conflict with CSUS campus policy that specifically restricted such independent domains, and did so without written exception from the campus. Further, daily and weekly backups for UEI systems were not stored at an off-site location, and the UEI information technology disaster recovery plan did not reference the CBORD, Active Directory and email systems.

UNIVERSITY ENTERPRISES DEVELOPMENT GROUP

FACILITIES AGREEMENTS [31]

Certain sublease agreements between the University Enterprises Development Group and third parties did not include appropriate indemnification provisions.

CAPITAL PUBLIC RADIO, INC.

OPERATING AND ADMINISTRATIVE AGREEMENTS [33]

Capital Public Radio, Inc. (CPR) was not fulfilling any of the authorized functions of California State University auxiliary organizations nor contributing to the educational mission of the university, and it had received annual payments from the campus general fund for services that were required by its operating agreement.

OPERATIONAL COMPLIANCE [35]

CPR had not developed a comprehensive written risk management policy.

FEES, REVENUES, AND RECEIVABLES [36]

Administration of CPR pledges receivable needed improvement, as collection activity and follow-up on delinquent pledges receivable was not adequate to ensure collection; management review of the pledges receivable aging report was not documented; long outstanding pledges receivable were not written off in a timely manner; and policies and procedures had not been documented for the monitoring of pledges receivable, collection of delinquent pledges, and write-off of uncollectible pledges. Also, CPR's

administration of corporate matching gifts needed improvement, as documentation was not maintained to show evidence that gifts were evaluated for eligibility of matching, subjected to a dual review to ensure that funds are administered in accordance with corporate donor requirements, and deposited as directed in a timely manner. Additionally, matching gifts auto-added pledges were erroneously processed and recorded as accounts receivable, and there was no follow-up and/or write-off of aged outstanding corporate matching gift pledges. Some elements are repeat findings from the prior Auxiliary Organizations audit.

INFORMATION TECHNOLOGY [39]

CPR did not ensure that credit card information was stored and transmitted in compliance with Payment Card Industry (PCI) Data Security Standard (DSS) requirements, and password controls and data security were not always adequate for CPR systems. Also, CPR did not perform a periodic, documented management review of user access privileges within all critical systems and applications containing protected data. CPR domain administration needed improvement, as an independent Active Directory domain was operated without written exception from the campus and password security parameters were inadequate for the domain controller. Further, CPR operated an independent network not part of the campus networking infrastructure that had not been authorized by campus IRT. In addition, CPR employees with access to critical systems or protected data were not required to complete information security awareness training. Finally, CPR had not completed a comprehensive information technology disaster recovery plan. Some elements are repeat findings from our Information Security audit conducted in July 2009.

ASSOCIATED STUDENTS OF CALIFORNIA STATE UNIVERSITY, SACRAMENTO

OPERATIONAL COMPLIANCE [48]

The Associated Students of California State University, Sacramento (ASI) had not developed written policies and procedures to address the accounting and processing of accounts receivable.

SEGREGATION OF DUTIES [48]

Certain duties and responsibilities related to accounts payable processing were not adequately segregated at ASI.

CASH RECEIPTS AND HANDLING [49]

Checks received at ASI were neither adequately safeguarded nor deposited in a timely manner, and accountability for cash receipts was not always localized to a specific employee.

FEES, REVENUES, AND RECEIVABLES [51]

Management review of ASI accounts receivable reconciliations was not documented.

PERSONNEL AND PAYROLL [52]

ASI employee timesheets were not always approved prior to payroll processing.

PROPERTY AND EQUIPMENT [52]

Administration of ASI property and equipment needed improvement, as an independent physical inventory of all property and equipment was not performed, review of monthly reconciliations of the property sub-ledger to the general ledger was not documented, and property and equipment was not consistently tagged.

INFORMATION TECHNOLOGY [54]

Password controls and data security were not always adequate for ASI systems.

UNIVERSITY UNION OPERATION OF CALIFORNIA STATE UNIVERSITY, SACRAMENTO

OPERATING AND ADMINISTRATIVE AGREEMENTS [56]

The University Union Operation of California State University Sacramento (Union) performed a function not authorized by its operating agreement with the CSU Trustees, specifically, the administration of stipends.

PURCHASING AND ACCOUNTS PAYABLE [57]

The Union did not recover a refundable deposit paid in advance for a Union-sponsored trip.

PROPERTY AND EQUIPMENT [57]

Administration of Union property and equipment did not provide for completion of the physical inventory in a timely manner, timely recording of additions and disposals to fixed asset records, timely recording of related depreciation expense to the general ledger, and timely reconciliation of fixed assets accounts to the general ledger.

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 at Sacramento State

The University Foundation at Sacramento State (Foundation) was established in 1986 as a non-profit public benefit corporation to act as the university's primary philanthropic function and to actively support the university's mission of teaching, learning, and service by acquiring and managing financial and other resources for the university. The Foundation is governed by a board of directors composed of student, faculty, university administration, and community members. The Foundation relies on

University Enterprises, Inc. personnel for accounting support services and relies on the campus for administrative and IT services.

University Enterprises, Inc.

University Enterprises, Inc. (UEI) was established in 1951 as a non-profit public benefit corporation to manage an array of programs and services that support and strengthen the university's mission of teaching, scholarship, and public services. UEI is responsible for administering dining and vendor services, bookstore operations, the copy graphic center, and Upper Eastside Lofts, as well as providing accounting services. UEI has outsourced the bookstore operations and Upper Eastside Lofts to third-party vendors. In addition to these operations, UEI is responsible for grant and contract management and fiscal services for university research and sponsored programs. It also provides fiscal services to university-related agencies and activities. UEI is the largest employer of student jobs, both on and off campus, throughout the State of California. Further, numerous state agencies and private employers use UEI's student employment services as their source for student assistants. UEI is governed by a board of directors composed of student, faculty, university administration, and community members. UEI provides accounting services to the Foundation, University Union Operation of California State University, Sacramento, and University Enterprises Development Group.

University Enterprises Development Group

University Enterprises Development Group (UEDG) was established in 2005 as a non-profit public benefit corporation responsible for the purchase, development, provision, maintenance, or sale of property and facilities, including the provision of affordable housing and other related facilities and activities, for the university's faculty, staff, and students. UEDG works to foster an academic community and environment near the campus and to attract and retain the highest quality faculty, staff, and students. UEDG is governed by a board of directors composed of representatives from the university and UEI auxiliary administration. UEDG does not have employees and relies on UEI personnel for all accounting and business administration services.

Capital Public Radio, Inc.

Capital Public Radio, Inc. (CPR) was established in 1970 as a student-operated station on the campus of California State University, Sacramento as radio station KERS. CPR was incorporated as an auxiliary organization of the CSU in 1991 and currently operates as a non-profit public benefit corporation that broadcasts classical music, jazz, news, public affairs, and locally produced specialty programs. CPR seeks to provide a trusted source of information, music, and entertainment for its listeners while strengthening the civic and cultural life of the communities it serves. CPR is governed by a board of directors composed of representatives from the community, university administration, faculty, a student, and CPR's president and general manager.

Associated Students of California State University, Sacramento

Associated Students of California State University, Sacramento (ASI) was established in 1956 as a non-profit public benefit corporation to provide support to a variety of programs aimed at meeting the needs

of the students of the university. The ASI also serves as a vehicle for participation of students in the governance of the university and as the fiscal agent for deposit accounts for student organizations and other student-related programs and activities. ASI is governed by a board of directors composed of representatives from the community, university administration, faculty, current students, alumni, and the campus president.

University Union Operation of California State University, Sacramento

University Union Operation of California State University, Sacramento (Union) was established in 1975 as a non-profit public benefit corporation to promote and assist the university's educational programs. The Union provides a central space for students, faculty, staff, alumni, and the greater community to participate in campus life. The Union hub offers dining, activities, and meeting rooms. Additionally, the Union is responsible for the Well facilities, which opened in 2010. The Well offers recreational facilities to students, faculty, staff, and alumni. The Union is governed by a board of directors composed of representatives from the university administration, students, faculty, alumni, and an ASI representative. The Union does not have employees and has outsourced accounting services to ASI and payroll and personnel services to UEI.

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 2008/09 and 2009/10 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, 2010, to February 18, 2011. 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 at Sacramento State

- ▶ Operating and Administrative Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Endowment Administration
- ▶ Information Technology

University Enterprises, Inc.

- ▶ 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
- ▶ Auxiliary Programs
- ▶ Information Technology

University Enterprises Development Group

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Property and Equipment
- ▶ Auxiliary Programs

Capital Public Radio, Inc.

- ▶ 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
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Auxiliary Programs
- ▶ Information Technology

Associated Students of California State University, Sacramento

- ▶ 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

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

- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Information Technology

University Union Operation of California State University, Sacramento

- ▶ 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
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Property and Equipment
- ▶ Information Technology

Campus

- ▶ Campus Oversight and Control

We have not performed any auditing procedures beyond February 18, 2011. 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

FISCAL COMPLIANCE

The campus had not required full reimbursement by the auxiliaries for indirect costs incurred by the campus for public safety and information resources and technology (IRT) support services provided to the auxiliaries.

We reviewed auxiliary cost allocation plan documentation for fiscal years (FY) 2008/09, 2009/10, and 2010/11 and found that:

- ▶ In FY 2008/09, 25 percent of public safety costs were invoiced to the auxiliaries for reimbursement.
- ▶ In FY 2009/10, 50 percent of public safety costs and 50 percent of newly implemented IRT costs were invoiced to the auxiliaries for reimbursement.
- ▶ In FY 2010/11, 75 percent of public safety costs were invoiced to the auxiliaries for reimbursement.

Executive Order (EO) 1000, *Delegation of Fiscal Authority and Responsibility*, dated July 1, 2007, states that the campus president shall ensure that costs incurred by the California State University (CSU) Operating Fund for services, products, and facilities provided to other CSU funds and to auxiliary organizations are properly and consistently recovered with cash and/or a documented exchange of value. Allowable direct costs incurred by the CSU Operating Fund shall be allocated and recovered based on actual costs incurred. Allowable and allocable indirect costs shall be allocated and recovered according to a cost allocation plan that utilizes a documented and consistent methodology including identification of indirect costs and a basis for allocation. The campus chief financial officer, or designee, shall annually approve and implement the cost allocation plan.

The campus associate vice president for financial services stated that in an effort to allow the auxiliary organizations time to appropriately budget for increased reimbursement amounts, the cost allocations were prorated and incrementally increased over a four-year period.

Failure to require full reimbursement of indirect costs incurred by the campus increases the risk that the campus operating fund will not be fully compensated for support provided to auxiliary enterprises.

Recommendation 1

We recommend that the campus require full reimbursement by the auxiliaries for indirect costs incurred by the campus for public safety and IRT support services provided to the auxiliaries.

Campus Response

We concur. As of the 2011/12 fiscal year, the campus will require full reimbursement by the auxiliaries for indirect costs incurred by the campus for public safety and IRT support services provided to the auxiliaries. By October 31, 2011, cost allocation memos and invoices will be distributed to the auxiliary organizations.

CAMPUS OVERSIGHT AND CONTROL

The interrelationship between Capital Public Radio, Inc. (CPR), Capital Public Radio Endowment, Inc. (CPRE), and Tower 91, Inc. (T91), may provide unacceptable risk to the campus and the CSU.

CPR was closely affiliated with the following 501(c)3 organizations:

- ▶ CPRE, a nonprofit public benefit corporation whose sole purpose is to provide funding to CPR. CPR is the only beneficiary of the endowment, according to the CPRE bylaws.
- ▶ T91, a nonprofit public benefit corporation that holds title to the property where a CPR transmitting tower is located. It exists for the sole benefit of CPR.

Specifically, we found that CPR:

- ▶ Shared common board members with both nonprofit organizations.
- ▶ Exercised management and accounting oversight for both organizations.
- ▶ Filed tax returns on behalf of both organizations.
- ▶ Consolidated the other entities into the CPR financial statements.
- ▶ Allowed use of the auxiliary and the campus' name.
- ▶ Did not have a written agreement supporting the business arrangement with either organization.

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 organizational management structures be clearly defined and approved, and that business arrangements be supported by complete, written agreements.

The CPR chief financial officer (CFO) stated that CPRE was an entity created by a group of private donors to establish a fund that would benefit the station, and the assets stemmed from estate gifts to the station and special fund-raising done for the benefit of the endowment. Additionally, he stated that T91 was created in 1984 and was established to support the operations of CPR; it holds title to the land that houses CPR's KXJZ tower and has not reported any commercial activity for several years.

The lack of a clearly defined and approved organizational structure supported by complete written agreements between CPR, CPRE, and T91 exposes the campus and the CSU system to regulatory and legal consequences.

Recommendation 2

We recommend that the campus evaluate the relationship between CPR and the other nonprofit organizations to ensure that the current structure is appropriate and authorized by the CSU and campus and to identify and address potential risks associated with the relationships.

Campus Response

We concur. During August 2011, the campus created a CPR task force, whose mission is to develop recommendations for the president associated with the appropriate placement of CPRE and T91 in relationship with the university and CPR. Based on those results, the campus will implement the appropriate organizational structure and develop the necessary documentation and agreements.

The recommendations of the CPR task force will be submitted to the campus president by January 31, 2012. Task force membership consists of CPR president and general manager, CPR CFO, chair of CPR board of directors, vice president for university advancement, associate vice president for business and administrative services, and campus auditor.

INFORMATION TECHNOLOGY

PASSWORD SECURITY

Password controls were not adequate for donor systems administered by the campus.

We found that all users in the Advance donor system and the SmartCall telefundraising system were assigned the same password that users could not change. Further, password expiration was not enforced, and users had to contact campus IRT to request password changes.

California State University, Sacramento (CSUS) Access Control Standard: 8060.0 Revised: August 15, 2010, states that all campus password management is carried out under the authority of the information security officer. All passwords must have a minimum length of any 15 U.S. keyboard characters, with the passphrase being the preferred method for achieving this length. Those having elevated access to confidential information (e.g. access control administrators, systems administrators, etc.) are encouraged to use longer passphrases.

Integrated California State University Administrative Manual (ICSUAM) §8045.100, *Information Technology Security*, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take

reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

The campus information security officer stated that the Advance and SmartCall systems had not been identified to be included in the campuswide authentication system because the systems were not capable of using the preferred method of common authentication. He further stated that IRT was unaware that shared passwords were being used for the Advance system.

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

Recommendation 3

We recommend that the campus set password security parameters for the donor systems in accordance with campus policy and perform an assessment of password security parameters for all other campus systems used by auxiliary organizations.

Campus Response

We concur. By December 31, 2011, the campus will integrate the donor systems into established campuswide controls. Additionally, the campus will perform and document an assessment of password security parameters for all other campus systems used by auxiliary organizations and implement appropriate password controls.

DISASTER RECOVERY PLAN

The campus information technology (IT) disaster recovery plan (DRP) did not include adequate details for the recovery of the donor systems.

ICSUAM §8085, *Business Continuity and Disaster Recovery*, states that an information security program needs to support the maintenance and potential restoration of operations through and after both minor and catastrophic disruptions. Campuses must ensure that their information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users. Each campus must maintain an ongoing program that ensures the continuity of essential functions and operations following a catastrophic event.

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 campus vice president and chief information officer (CIO) stated that the campus had determined that donor systems did not need to be included in the IT DRP because advancement is not an essential business function and is not critical to university operations. He further stated that campus IRT indicated that the campus DRP covers only a few mission critical computer systems that must be brought back online within 24 hours, and that non-mission critical campus systems, including donor systems, are subject to secondary business continuity planning that identifies alternate means of conducting activity until secondary systems can be brought back online. Finally, he stated that secondary systems may be offline for up to two weeks in a disaster, but business continuity planning done in the business unit allows donor activity to continue.

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 4

We recommend that the campus update the IT DRP to include adequate details for the recovery of the donor systems.

Campus Response

We concur. By December 31, 2011, the campus will update the IT DRP to include adequate details regarding the expectation for recovery of the donor systems, consistent with the recovery expectations for other non-mission critical systems.

THE UNIVERSITY FOUNDATION AT SACRAMENTO STATE

OPERATIONAL COMPLIANCE

RISK MANAGEMENT

The University Foundation at Sacramento State (Foundation) had not developed a comprehensive written risk management policy.

We found that the Foundation did not have a comprehensive written risk management policy that addressed an ongoing process to proactively identify risks, analyze the frequency and severity of identified risks, and implement a risk mitigation program that coordinates with the campus' risk assessment and mitigation plan.

EO 715, *California State University Risk Management Policy*, dated October 27, 1999, delegated authority and responsibility to the campus president to implement campus risk management policies consistent with the CSU Risk Management Policy guidelines. This includes an ongoing process to identify risks, analyze the frequency and severity of the potential risks, and select the best management techniques to manage the risks.

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 8.7, *Risk Management*, states that auxiliary organizations should develop programs to manage risk related to activities in which the organizations are engaged.

The campus vice president of university advancement stated that the Foundation relied upon the campus for risk management and therefore had assumed that the campus risk management policy included reference to Foundation operations.

The absence of a comprehensive risk management policy increases the likelihood that all current risk-related activities may not be adequately evaluated.

Recommendation 5

We recommend that the Foundation develop and adopt a comprehensive written risk management policy that includes procedures to actively identify, analyze, quantify, and manage risk.

Campus Response

We concur. By December 31, 2011, the Foundation will develop and adopt a comprehensive written risk management policy that includes procedures to actively identify, analyze, quantify, and manage risk.

CONFLICT OF INTEREST

The Foundation had not obtained annual conflict of interest statements from all board members.

We found that two of the 18 board members had not signed a conflict of interest statement for FY 2009/10.

CSU Conflict of Interest Handbook, §2B, states that the Political Reform Act requires CSU to adopt a formal conflict of interest code. The CSU's code requires certain employees, who are most likely to be involved in university decision-making where potential conflicts may be present, to file an annual disclosure form.

Title 5 §42401, §42402, §42500 and Education Code §89900 establish a responsibility to operate in accordance with sound business practices in the interest of the campus. Sound business practice mandates establishing conflict of interest policies and procedures and compliance with existing policies and procedures.

The vice president of university advancement stated that the two board members joined later in the fiscal year and therefore did not complete their conflict of interest forms during the annual acknowledgement process.

Failure to obtain conflict of interest statements from all auxiliary board members annually increases liability for acts contrary to the code.

Recommendation 6

We recommend that the Foundation obtain annual conflict of interest statements from all board members.

Campus Response

We concur. As of June 2011, the Foundation board obtained the conflict of interest statements from all members serving during 2011/12.

UNIVERSITY ENTERPRISES, INC.

OPERATING AND ADMINISTRATIVE AGREEMENTS

Certain agreements between University Enterprises, Inc. (UEI) and third parties did not include appropriate provisions for indemnification or the right to audit.

We reviewed 11 food service vendor agreements, one outsourced bookstore operating agreement, and six sponsored programs sub-award agreements and found that:

- ▶ Six food service vendor agreements did not indemnify the State of California.
- ▶ Two food service vendor agreements did not include the right to audit.
- ▶ One outsourced bookstore operating agreement did not indemnify the state of California.
- ▶ Six sponsored programs sub-award agreements exceeding \$10,000 did not contain a provision that the contracting parties shall be subject to the examination and audit of the auxiliary and its agents.

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.

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 sub-award agreements contain a provision for the right to audit.

The UEI director of property services stated that the vendor agreements did not indemnify the state of California as a result of a typographical error made during the revision process. The UEI director of dining services stated that two food service vendor agreements did not include right to audit

provisions due to oversight. The UEI director of contract and research administration stated that UEI was unaware that the sub-award agreements exceeding \$10,000 had to contain a provision indicating that the contracting parties shall be subject to the examination and audit of the auxiliary and its agents.

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

Recommendation 7

We recommend that UEI:

- a. Amend the cited agreements with appropriate indemnification and right to audit provisions.
- b. Ensure all future agreements include appropriate indemnification and right to audit provisions.

Campus Response

We concur. UEI will revise the cited agreements to include the appropriate indemnification and right to audit provisions. Additionally, UEI will revise its lease and sub-award agreement templates to contain the appropriate indemnification and right to audit provisions. These actions will be completed by September 30, 2011.

FEES, REVENUES, AND RECEIVABLES

UEI administration of sales revenues audits for the outsourced food and dining services vendors needed improvement.

We found that:

- ▶ UEI had not developed written policies and procedures for periodic audits of the outsourced vendors' sales revenues for verification of accurate commissions paid to UEI.
- ▶ Sales audits were completed for 11 of 15 total vendors in 2009 and 2010, but audits had not been completed for three vendors since 2006 and one vendor since 2008.
- ▶ Sales audits were performed by an employee who also managed the vendor relationship and reconciled monthly commissions.

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 8.9.4, *Receivables*, states that the auxiliary should establish a written internal controls system that ensures billing, cash collection, customer inquiries, and subsidiary reconciliations are conducted separately and with due regard for the receivable duties.

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 development of policies and procedures for periodic audits of outsourced vendors' sales revenues, completion of sales audits in a timely manner, and performance of sales audits by an independent person.

The UEI director of dining services stated that duties related to the audit of sales revenues of the outsourced food and dining services had not been reassigned when a staff member left. In addition, he stated that the business analyst of dining services performed the audit as her own internal process but was not able to perform the audits every year due to staffing and workload issues. He also stated that three vendors had not been audited since 2006 because two had been identified as low-risk vendors and another ceased operation in May 2010.

The absence of written policies and procedures increases the risk that errors, inconsistencies, or misunderstandings will occur, and untimely performance of sales audits by a non-independent person increases the risk that errors and irregularities will not be detected in a timely manner and increases the risk of misappropriation.

Recommendation 8

We recommend that UEI:

- a. Develop written policies and procedures to periodically audit the sales revenues of the outsourced food and dining services to verify the accuracy of sales commission paid to UEI.
- b. Complete sales audits in a timely manner.
- c. Ensure that sales audits are completed by an independent person.

Campus Response

We concur. Effective June 2011, the following was implemented:

- a. UEI developed and implemented a written policy, *Dining Services/Business Services Vendors' Sales and Commission Audit*, and procedures for the performance of periodic audits of the sales revenues of the outsourced food and dining services to verify the accuracy of sales commissions paid to UEI. A component of these procedures includes the completion and review of a

spreadsheet listing the vendors and dates of sale revenue audits, along with the results of audits completed.

- b. A regular, rotating audit schedule was created to include five randomly selected vendors to be audited each fiscal year, with those audits covering a two month period. The timing of the audits is such that each vendor is guaranteed to be audited no less than once every two years. UEI's controller will review the spreadsheet calendar to ensure that all audits are completed by the prescribed dates.
- c. The completion of the sales audits was assigned to the accounts receivable department under the supervision of the controller, both independent parties, with assistance provided as necessary by dining services personnel.

AUXILIARY PROGRAMS

The UEI effort certification process did not consider other campus work assignments for faculty members. This is a repeat finding from the prior Auxiliary Organizations audit.

We found that although UEI reviewed timesheets prepared by the faculty members, the information was not compared to other campus work assignments. Without this critical information, the calculation of a faculty member's actual effort on a sponsored project cannot be determined.

Office of Management and Budget (OMB) Circular A-21, *Cost Principles for Educational Institutions*, §.J.10.b.(2)(b), states that the method of documenting the distribution of charges for personal services must recognize the principle of after-the-fact confirmation or determination so that costs distributed represent actual costs, unless a mutually satisfactory alternative agreement is reached. Direct cost activities and facilities and administration cost activities may be confirmed by responsible persons with suitable means of verification that the work was performed.

OMB Circular A-110, *Uniform Administrative Requirements for Grants and Agreements With Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations Financial Reporting*, §.71(a), states that recipients shall submit, within 90 calendar days after the date of completion of the award, all financial, performance, and other reports as required by the terms and conditions of the award.

The UEI director of contract and research administration stated that efforts were made to obtain campus work assignments but were delayed due to university report development and Common Management System access privileges. She further stated that access was given to her and the assistant director of administration and operations in December 2010.

Failure to consider all faculty work assignments in the effort certification process increases the risk of non-compliance with OMB requirements and exposes the auxiliary organization to penalties and disallowances for non-compliance with contracts and grants terms.

Recommendation 9

We recommend that UEI request faculty members' campus work assignments for inclusion in its calculation of the actual level of faculty effort provided to sponsored projects.

Campus Response

We concur. By March 31, 2012, RACA will develop and implement a procedure with relevant campus units to obtain and assess a copy of the faculty workload report for each new award. Copies of the workload report will be maintained on file.

INFORMATION TECHNOLOGY

DATA SECURITY AND ASSESSMENT

Protected and/or sensitive data was not encrypted when stored in the UEI accounting and payroll systems, and UEI did not perform an assessment and inventory of protected data residing on an administrative file server.

We found that:

- ▶ The IFAS financial and payroll systems contained sensitive employee data that was not encrypted.
- ▶ An administrative file server with shared drives for administrative, accounting, human resources/payroll, and sponsored programs was not encrypted, and an assessment and inventory of protected data on the server had not been conducted.

CSUS Supplemental Security Policy for Information Access Management, Policy Number: 8065.0 Revised: August 15, 2010, states that encryption of level 1 data in storage or prior to transmission may be required, to prevent the possibility of compromise, interception, or misrouting.

ICSUAM §8045.100, *Information Technology Security*, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

ICSUAM §8065, *Information Asset Management*, states that campuses must maintain an inventory of information assets containing level 1 or level 2 data as defined in the CSU Data Classification Standard. These assets must be categorized and protected throughout their entire life cycle, from origination to destruction.

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 security assessment of auxiliary systems and inventory of protected information residing on systems.

The UEI director of IT stated that encryption of the IFAS financial and payroll systems was not supported by the vendor and that an assessment and inventory of all protected data had been initiated but not completed due to competing priorities and resource constraints.

Failure to ensure that all sensitive information has been identified and properly secured increases the auxiliary's exposure to information security breaches and could result in the violation of legal statutes that could result in financial penalties and loss of public trust.

Recommendation 10

We recommend that UEI:

- a. Apply encryption controls to the financial and payroll systems and all other UEI systems, computers, databases, and file servers that house protected and/or sensitive data, or institute mitigating controls approved by the campus CFO.
- b. Perform an assessment of protected information residing on the administrative file server.

Campus Response

We concur.

- a. By December 31, 2011, UEI will apply applicable encryption or other mitigating controls to the financial and payroll systems and all other UEI systems, computers, databases, and file servers that house protected and/or sensitive data.
- b. As of July 2011, UEI conducted an assessment of each departmental drive, and assessments of all data storage will be performed on an annual basis.

NETWORK SECURITY

The UEI network did not place Internet-accessible web servers on a separate network segment from other production servers.

ICSUAM §8045.100, *Information Technology Security*, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

ICSUAM §8045.300, *Network Security*, states that campuses must appropriately design their networks—based on risk, data classification, and access—in order to ensure the confidentiality, integrity, and availability of their information assets. Each campus must implement and regularly review a documented process for transmitting data over the campus network. This process must include the identification of critical information systems and protected data that is transmitted through the campus network or is stored on campus computers. Campus processes for transmitting or storing critical assets and protected data must ensure confidentiality, integrity, and availability.

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 network segmentation to logically separate any protected data residing on internal auxiliary systems from Internet-accessible devices.

The UEI director of IT stated that network segmentation had been identified as a future project but had not been implemented because UEI does not have the authority to set up network subnets, as IRT is responsible for all network and infrastructure services.

Failure to separate and protect internal auxiliary resources from Internet-accessible devices increases the risk of internal network exposure to security compromises and inadequate security over information assets with protected data.

Recommendation 11

We recommend that UEI place Internet-accessible web servers on a separate network segment from other production servers.

Campus Response

We concur. By December 31, 2011, UEI will work with campus IRT to appropriately segment public-facing servers on the network.

DOMAIN ADMINISTRATION

UEI operated an independent Active Directory domain in conflict with CSUS campus policy that specifically restricted such independent domains, and did so without written exception from the campus.

CSUS Supplemental Security Policy for Access Control, Policy Number: 8060.0 Revised: August 15, 2010, states that all campus employees implementing and supporting authentication and access control processes must comply with the campus Access Control Standards, as defined by the information security officer. All account provisioning and deprovisioning campuswide must take place only under standards set by the information security officer and must use the defined campuswide identity management system. All accounts will be housed only in the unified University Active Directory domain, unless written exceptions are approved through the information security officer. All exceptions to the above access control policies must be approved in writing using the procedures identified in Section 8000.200.

The UEI director of IT stated that UEI had always operated an independent domain and was not fully aware of the recent campus policy requirements. She further stated that UEI had filed an exception to the CSUS access control policy during the audit.

Failure to comply with campus access control policy increases the risk of mismanaged domains operating on the campus network, which could result in security incidents that could compromise campus network resources.

Recommendation 12

We recommend that UEI house all user accounts in the unified Active Directory domain or obtain written exception from the campus.

Campus Response

We concur. UEI requested an exception to this security policy from the campus. This exception request is under review by the campus, and a determination will be made by December 31, 2011.

SYSTEM BACKUPS

Daily and weekly backups for UEI systems were not stored at an off-site location.

We found that backups were being retained in the server room inside a locked cabinet.

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 off-site storage of backups.

The UEI director of IT stated that backups were not stored off-site due to pending negotiations with a third-party contractor for off-site storage.

Failure to store backups at an off-site location increases the risk that auxiliary systems will not be recovered in the event of a disaster.

Recommendation 13

We recommend that UEI store backups at an off-site location.

Campus Response

We concur. As of March 2011, UEI tapes have been stored off-site on a weekly rotation via Access Information Management.

DISASTER RECOVERY PLAN

The UEI IT DRP did not reference the CBORD, Active Directory, and email systems.

ICSUAM §8085, *Business Continuity and Disaster Recovery*, states that an information security program needs to support the maintenance and potential restoration of operations through and after both minor and catastrophic disruptions. Campuses must ensure that their information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users. Each campus must maintain an ongoing program that ensures the continuity of essential functions and operations following a catastrophic event.

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 UEI director of IT stated that the IT DRP only included the financial system because it handles the bulk of the UEI data processing, and that other key UEI operations could operate manually without dedicated systems.

The absence of a comprehensive IT DRP inclusive of all critical auxiliary systems 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 14

We recommend that UEI update its IT DRP to include reference to the CBORD, Active Directory, and email systems.

Campus Response

We concur. By January 31, 2012, UEI will update disaster recovery documentation to include references to the CBORD, Active Directory, and email systems.

UNIVERSITY ENTERPRISES DEVELOPMENT GROUP

FACILITIES AGREEMENTS

Certain sublease agreements between the University Enterprises Development Group (UEDG) and third parties did not include appropriate indemnification provisions.

We found that the indemnification provisions in sublease agreements with a fitness center and a food vendor did not specifically indemnify the state of California, CSU Trustees, and the campus.

The CSURMA/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 UEI director of property services stated that indemnification clauses had not been used consistently in the past 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 15

We recommend that UEDG:

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

Campus Response

We concur. As of July 2011, UEI, the assignee of UEDG's agreements, obtained a signed lease amendment from the food operator reflecting the corrected indemnification provisions. As of August 2011, UEI submitted an amendment with corrected indemnification provisions to the fitness center for their signature, with the expectation that the signed amendment will be received by

December 31, 2011. The lease template used for all third-party leases was revised as of July 2011 and contains the correct indemnification provisions.

CAPITAL PUBLIC RADIO, INC.

OPERATING AND ADMINISTRATIVE AGREEMENTS

Capital Public Radio, Inc. (CPR) was not fulfilling any of the authorized functions of CSU auxiliary organizations nor contributing to the educational mission of the university, and it had received annual payments from the campus general fund for services that were required by its operating agreement.

We reviewed the CPR incorporation documents and operating agreements and found that:

- ▶ The CPR operating agreement stated that CPR was approved to operate a radio station and provide the university with advertising services, neither of which are listed among the essential functions of auxiliary organizations determined/authorized by the CSU Board of Trustees.
- ▶ CPR operations did not provide any instructionally related activities for the benefit of CSUS students.
- ▶ CPR was paid annually by the university from FY 2005/06 to 2007/08 through service orders for on-air identification. However, these on-air identification services were required, without remuneration, by CPR's operating agreement with the university. CPR was paid \$285,000 from the university general fund during these three fiscal years.

Title 5 §42500 states that auxiliary organizations are formed to provide essential functions which are an integral part of the educational mission of a campus and the California State University. Section (a)(8) further explains that radio and television stations have been determined by the Board to be appropriate for auxiliary organizations to perform in accordance with applicable policies, rules, and regulations within the function of instructionally related programs and activities.

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 1.1, *Mandatory Board of Trustees' Requirements for Auxiliary Organization Status*, states that the Board of Trustees, through the references indicated, has established certain characteristics that an organization must have in order to be qualified to become or continue to be a CSU auxiliary organization. Auxiliary organizations are those nonprofit organizations that: conduct campus activities "...essential to the educational program of a campus...and are an integral part of a campus program..."; have "...agreed to comply with the applicable requirements of the Board of Trustees and campus"; are "...included in the list of officially recognized auxiliary organizations in good standing maintained by the Chancellor..."; and "...maintain the status of an auxiliary organization in good standing."

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 17.2, *Self-Supporting*, states that service or commercial operations are required to be self-supporting. Traditionally, this has been interpreted to mean that surplus funds from one commercial operation are not to be used to fund the operations of another commercial operation. For example, a

campus bookstore operation must not subsidize a food service operation for a prolonged period unless there is a conscious decision by those individuals responsible for the oversight of these operations that this practice is in the best interest of the campus and its academic mission.

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 business arrangements be supported by complete, written agreements.

The CPR CFO stated his belief that CPR was performing its duties as an auxiliary as defined in its operating agreement with the Trustees. He further stated that the payments received from the university were assumed to be acceptable as general support since they were remitted by the university.

Failure to include and provide one of the pre-approved functions of auxiliary organizations within an auxiliary operating agreement increases the risk of misunderstandings and miscommunications regarding responsibilities, programs, and activities provided. Receiving funds from the university's general fund is not in the best interest of the campus and its academic mission and limits the auxiliary organization's ability to be a self-supporting entity.

Recommendation 16

We recommend that CPR:

- a. Amend its operating agreement to include an essential function of CSU auxiliary organizations determined/authorized by the CSU Board of Trustees.
- b. Provide instructionally related activities for the benefit of CSUS students.
- c. Decline payments from the university for service orders that are required to be performed without remuneration by its operating agreement with the university.

Campus Response

We concur. The campus and CPR will amend the CPR operating agreement to properly substantiate its essential function as a CSU auxiliary organization. The campus and CPR will provide relevant instructionally related activities for the benefit of CSUS students.

During August 2011, the campus created a CPR task force, whose mission is to develop recommendations for the president regarding revisions to the CPR operating agreement, in particular that the operating agreement will include an essential function of CSU auxiliary organizations as determined and authorized by the CSU Board of Trustees. Additionally, the task force will define

instructionally related activities and provide guidance regarding the implementation of instructionally related activities accessible to our students and associated with the operation of CPR.

The recommendations of the CPR task force will be submitted to the campus president by January 31, 2012. Task force membership consists of CPR president and general manager, CPR CFO, chair of CPR board of directors, vice president for university advancement, associate vice president for business and administrative services, and campus auditor.

Since 2008/09, CPR has not accepted any payments from the university related to service orders that are required to be performed without remuneration by its operating agreement with the university. Additionally, CPR will not accept any payments of this nature in the future.

OPERATIONAL COMPLIANCE

CPR had not developed a comprehensive written risk management policy.

We found that CPR did not have a comprehensive written risk management policy that addressed an ongoing process to proactively identify risks, analyzed the frequency and severity of identified risks, and implemented a risk mitigation program that coordinated with the campus' risk assessment and mitigation plan.

EO 715, *California State University Risk Management Policy*, dated October 27, 1999, delegated authority and responsibility to the campus president to implement campus risk management policies consistent with the CSU Risk Management Policy guidelines. This includes an ongoing process to identify risks, analyze the frequency and severity of the potential risks, and select the best management techniques to manage the risks.

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 8.7, *Risk Management*, states that auxiliary organizations should develop programs to manage risk related to activities in which the organizations are engaged.

The CPR CFO stated that due consideration has been given to the development of a risk management policy in conjunction with a business continuity and disaster recovery plan, but it had not been completed as CPR was still in the research and analysis phase of the project.

The absence of a comprehensive written risk management policy increases the likelihood that all current risk-related activities may not be adequately evaluated.

Recommendation 17

We recommend that CPR develop and adopt a comprehensive written risk management policy, including procedures to actively identify, analyze, quantify, and manage risk.

Campus Response

We concur. By December 31, 2011, CPR will develop and adopt a comprehensive written risk management policy that includes procedures to actively identify, analyze, quantify, and manage risk.

FEES, REVENUES, AND RECEIVABLES

ACCOUNTS RECEIVABLE

Administration of CPR pledges receivable needed improvement.

We reviewed ten pledges receivable from the pledges receivable aging report as of January 28, 2011, and found that:

- ▶ Collection activity and follow-up on delinquent pledges receivable was not adequate to ensure collection. CPR had not documented collection correspondence and did not address further action to be taken on delinquent pledges.
- ▶ Management review of the pledges receivable aging report was not documented.
- ▶ Long outstanding pledges receivable were not written off in a timely manner.
- ▶ Policies and procedures had not been documented for the monitoring of pledges receivable, collection of delinquent pledges, and write-off of uncollectible pledges.

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 8.9.4, *Receivables*, states that the auxiliary should establish a written system to invoice customers promptly, in a consistent manner, while exercising due diligence in the follow-up and collection of past-due accounts.

The CPR CFO stated that current procedures did not call for retention of collection activity and documentation of management's review of aging reports. He further stated that the failure to write off outstanding pledges receivable and develop written policies and procedures for monitoring pledges receivable, collection of delinquent pledges receivable, and write-off of uncollectible pledges was due to oversight.

Inadequate administration over pledges receivable increases the risk that receivables will not be properly controlled and accurately reflected in auxiliary financial statements, reduces the likelihood of collection, and negatively impacts cash flow.

Recommendation 18

We recommend that CPR:

- a. Promptly pursue the collection of delinquent pledges receivable.
- b. Document managerial review of the pledges receivable aging report.
- c. Write off long outstanding pledges receivable in a timely manner.
- d. Document policies and procedures for the monitoring of pledges receivable, collection of delinquent pledges, and write-off of uncollectible pledges.

Campus Response

We concur. By December 31, 2011, CPR will complete the following:

- a. CPR will develop and implement procedures to promptly pursue the collection of delinquent pledges receivable.
- b. CPR will develop and implement procedures related to the required documentation of the managerial review of the pledges receivable aging report.
- c. CPR will develop and implement procedures related to the write-off of long outstanding pledges receivable in a timely manner.
- d. CPR will develop and implement policies and procedures for the monitoring of pledges receivable, collection of delinquent pledges, and write-off of uncollectible pledges.

MATCHING GIFTS

Administration of CPR corporate matching gifts needed improvement.

We found that:

- ▶ Corporate matching gift documentation was not maintained to show evidence that gifts were evaluated for eligibility of matching, subjected to a dual review to ensure that funds are administered in accordance with corporate donor requirements, and deposited as directed in a timely manner. This is a repeat finding from the prior Auxiliary Organizations review.
- ▶ Matching gifts auto-added pledges were erroneously processed and recorded as pledges receivable. The pledges receivable aging report as of January 28, 2011, showed that auto-added pledges, established on the basis of an existing relationship, were erroneously recorded and aged as outstanding receivables. The system permitted matching gift pledges to be auto-added, even though a pledge had not been requested by the constituent. Moreover, the auto-added pledges were not tracked, reviewed, or scrutinized, and consequently, they remained outstanding for more than 360 days and required manual correction.

- ▶ There was no follow-up and/or write-off of aged outstanding corporate matching gift pledges. This is a repeat finding from the prior Auxiliary Organizations audit.

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 that 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.

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 8.9.4, *Receivables*, states that the auxiliary should properly record and promptly collect receivables in a consistent manner utilizing systems that ensure integrity of existing internal controls.

The CPR Matching Gifts policy states that all pledges that are 12 months past due or have no donor-directed activity within a 12-month period will be written off as uncollectible. The write-off will be noted in the donor's Raiser's Edge account.

The CPR CFO stated that there were several changes in the membership director position over the past three years, and the turnover resulted in the failure to follow up on the findings from the last audit and other matching gift concerns.

Inadequate administration of matching gifts increases the likelihood that funds will be misdirected and the campus will be exposed to liabilities from non-compliance with corporate donor policies.

Recommendation 19

We recommend that CPR:

- a. Maintain documentation of matching gift dual review in support of the evaluation and receipt of corporate matching gifts to ensure that funds are administered in accordance with corporate donor requirements and deposited as directed in a timely manner.

- b. Manually correct/write-off auto-added pledges, disable the auto-added feature within the database, and ensure that pledges are entered at the constituents' requests.
- c. Follow-up and/or write-off aged outstanding matching gifts.

Campus Response

We concur. By December 31, 2011, CPR will improve the administration of corporate matching gifts:

- a. CPR will develop and implement procedures related to corporate matching gifts. At a minimum, these procedures will address the retention of documentation to evidence that gifts were evaluated for eligibility of matching, were subjected to a dual review to ensure that funds were administered in accordance with corporate donor requirements, were deposited as directed and in a timely manner, and ensure that only pledges based on constituents' requests are entered in to the database.
- b. CPR will write-off the auto-added pledges and will disable the auto-added feature within the database. Based on newly implemented procedures, CPR will ensure that pledges are entered based on the constituents' requests.
- c. CPR will write-off outstanding matching gifts that are more than 12 months past due or had no donor-directed activity within the past 12 months. The write-off information will be noted in the donor's account, using Raiser's Edge.

INFORMATION TECHNOLOGY

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD COMPLIANCE

CPR did not ensure that credit card information was stored and transmitted in compliance with Payment Card Industry (PCI) Data Security Standard (DSS) requirements.

We found that:

- ▶ Credit card information stored in paper form that was used to process recurring monthly membership charges was not redacted, locked when not in use, or discarded immediately after successful processing. Also, the files were accessible to all CPR employees, contractors, and volunteers.
- ▶ Workstations used to enter credit card data into the Raiser's Edge online system were not behind a PCI DSS-compliant firewall. Specifically, firewall rules did not deny all inbound and outbound traffic, and outbound traffic was not regulated by a proxy server as required by PCI DSS.

CPR Sensitive Information Handling policy, Section 4.A.2, *Hard Copy Distribution*, states that file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.

CPR Sensitive Information Handling policy, Section 4.A.3, *Electronic Distribution*, states in part that all sensitive information must be encrypted when stored in an electronic format.

ICSUAM §8045.100, *Information Technology Security*, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

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. PCI DSS prohibit the unencrypted storage of full credit card numbers, cardholder names, service codes, and expiration dates; and prohibit any storage, whether encrypted or not, of the three-digit security codes.

The CPR CFO stated that the current procedures to protect sensitive information had been considered adequate and that CPR was aware of the firewall deficiency but had not yet taken corrective action.

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 20

We recommend that CPR:

- a. Redact and adequately secure credit card information when not in use, or discard the information immediately after successful processing.
- b. Ensure PCI DSS-compliant configuration on the CPR firewall that protects the workstations used to enter credit card data into the Raiser's Edge online system.

Campus Response

We concur. By December 31, 2011, CPR will complete the following:

- a. CPR will work with the campus information security officer to complete a full assessment and analysis of CPR's compliance with the latest PCI standards. Based on the results of that assessment and analysis, CPR will develop and implement procedures required by those PCI standards applicable to the campus, and the procedures will include when to redact and secure credit card information when not in use and when to discard the information immediately after successful processing.
- b. CPR will work with campus IRT to develop and implement a PCI DSS-compliant configuration on the campus firewalls and CPR workstations and systems used to enter and process credit card data into the Raiser's Edge online system.

PASSWORD AND DATA SECURITY

Password controls and data security were not always adequate for CPR systems.

We found that:

- ▶ Password security parameters were inadequate for the Sage Business Works accounting system, as there was no minimum password length, password expiration, or automatic sign-off of users after a period of no use, nor were there complexity requirements or restrictions for reuse of passwords or access after repeated failed attempts.
- ▶ Protected and/or sensitive data was not encrypted when stored in the Sage Business Works accounting and Raiser's Edge donor systems.

CSUS *Supplemental Security Policy for Access Control*, Policy Number: 8060.0 Revised: August 15, 2010, states that adequate password management is a critical aspect of access control. All campus password management is carried out under the authority of the Information Security Officer. All passwords must have a minimum length of any 15 U.S. keyboard characters, with the passphrase being the preferred method for achieving this length. Those having elevated access to confidential information (e.g., access control administrators, systems administrators, etc.) are encouraged to use longer passphrases. All SacLink passwords must also be changed at least annually; passwords with elevated access and privileges to the campus fiscal system must be changed every 120 days, managed using the official campus password management system found at password.csus.edu.

ICSUAM §8045.100, *Information Technology Security*, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

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 and encryption of any protected/sensitive data residing on auxiliary systems.

The CPR CFO stated that the Sage Business Works system did not have automated password enforcement settings and that the encryption of protected and/or sensitive data was not possible with the current versions of the Sage Business Works and Raiser's Edge systems.

Inadequate password and login parameters may compromise the authentication credentials of user account privileges that are embedded into applications and operating systems, which in turn may increase the risk of unauthorized access to auxiliary systems and confidential data. 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 21

We recommend that CPR:

- a. Set effective password and login security parameters for the Sage Business Works accounting system in accordance with campus password guidelines, or institute mitigating controls approved by the campus CFO.
- b. Apply encryption controls to the accounting and donor systems and all other CPR systems, computers, databases, and file servers that house protected and/or sensitive data.

Campus Response

We concur. By December 31, 2011, CPR will complete the following:

- a. CPR will work with the campus information security officer to set and implement applicable campus standards for password and login security for Sage Business Works.
- b. CPR will apply applicable encryption or other mitigating controls to the accounting and donor systems and all other CPR or campus systems, computers, databases, and file servers that house and process protected and/or sensitive data. CPR will work with the campus information security officer to complete an assessment and analysis of servers handling sensitive data, to determine if those servers should be housed in the secure campus data center.

USER ACCESS REVIEW

CPR did not perform a periodic, documented management review of user access privileges within all critical systems and applications containing protected data.

ICSUAM §8060.400, *Access Control*, states that campuses must develop procedures to detect unauthorized access and privileges assigned to authorized users that exceed the required access rights needed to perform their job functions. Appropriate campus managers and data owners must review, at least annually, user access rights to information assets containing protected data. The results of the review must be documented.

The CPR CFO stated that documented management reviews were not completed due to oversight.

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 22

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

Campus Response

We concur. By December 31, 2011, CPR will work with campus IRT to develop and implement policies and procedures regarding the documented management reviews of user access privileges for all critical systems and applications containing protected data. The user access review will be conducted on an annual basis. These policies and procedures will be in compliance with campus policies and procedures.

DOMAIN ADMINISTRATION

CPR domain administration needed improvement.

We found that:

- ▶ CPR operated an independent Active Directory domain without written exception from the campus.
- ▶ Password security parameters were inadequate for the domain controller, as the minimum password length was set to only seven characters.

CSUS Supplemental Security Policy for Access Control, Policy Number: 8060.0 Revised: August 15, 2010, states that all campus employees implementing and supporting authentication and access control processes must comply with the campus Access Control Standards, as defined by the

information security officer. All account provisioning and deprovisioning campuswide must take place only under standards set by the information security officer and must use the defined campuswide identity management system. All accounts will be housed only in the unified University Active Directory domain, unless written exceptions are approved through the information security officer. All exceptions to the above access control policies must be approved in writing using the procedures identified in Section 8000.200.

ICSUAM §8080, *Physical Security*, 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. Campus information assets that can access protected data and are 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.

CSUS *Supplemental Security Policy for Access Control*, Policy Number: 8060.0 Revised: August 15, 2010, states that adequate password management is a critical aspect of access control. All campus password management is carried out under the authority of the information security officer. All passwords must have a minimum length of any 15 U.S. keyboard characters, with the passphrase being the preferred method for achieving this length. Those having elevated access to confidential information (e.g., access control administrators, systems administrators, etc.) are encouraged to use longer passphrases. All SacLink passwords must also be changed at least annually; passwords with elevated access and privileges to the campus fiscal system must be changed every 120 days, managed using the official campus password management system found at password.csus.edu.

The CPR CFO stated that CPR's Active Directory domain is specific to its broadcasting functions and needs to be maintained by radio station staff. He added that campus IRT is aware of this and charges CPR for additional information risk and non-compliance services. He also stated that CPR management was unaware of the need to apply for a written exception.

Failure to comply with campus access control policy increases the risk of mismanaged domains operating on the campus network, which could result in security incidents that could compromise campus network resources.

Recommendation 23

We recommend that CPR house all user accounts in the unified Active Directory domain or apply for written exception from the campus, in accordance with campus policy.

Campus Response

We concur. By December 31, 2011, CPR will work with the campus information security officer to maintain all user accounts in the campus unified Active Directory domain.

NETWORK ADMINISTRATION

CPR operated an independent network not part of the campus networking infrastructure that had not been authorized by campus IRT.

CSUS *Supplemental Security Policy for Network Security*, Standard Number 8045.0: Revised August 15, 2010, states that due to the critical nature of the campus networking infrastructure, the Networking and Telecommunication Services department of the Information Resources and Technology division is chartered to be the official owner of all campus network infrastructure, encompassing all wired jacks, network closets, (ip)PBXs, wireless access points, airwaves, and other aspects of networking. All defined network infrastructure devices must be registered with the ISO and specifically authorized for use as part of the campus network infrastructure by both the ISO and NTS departments. A network infrastructure device is any device implemented for the purpose of allowing faculty, staff, students, or third parties to access networked campus services. A network device maybe a router, switch, wireless access point, firewall, VOIP device, VPN, or other network appliance.

The CPR CFO stated that CPR's independent network is specific to its broadcasting functions and needs to be maintained by radio station staff. He further stated that campus IRT is aware of this and charges CPR additional fees for additional information risk and non-compliance services. He also stated that CPR management was unaware of the need to apply for written exception.

Failure to comply with campus network security policy increases the risk of mismanaged networks operating in conjunction with the campus network infrastructure, which could result in security incidents that could compromise campus network resources.

Recommendation 24

We recommend that CPR ensure that all network infrastructure devices are registered with the campus information security officer and specifically authorized for use as part of the campus network infrastructure, or apply for written exception from the campus information security officer for the operation of an independent network.

Campus Response

We concur. By December 31, 2011, CPR will work with campus IRT to register all network devices, to ensure compliance with all campus infrastructure security policies, and to apply for a written exception to operate applicable independent network segments.

INFORMATION SECURITY AWARENESS TRAINING

CPR employees with access to critical systems or protected data were not required to complete information security awareness training. This is a repeat finding from our Information Security audit conducted in July 2009.

ICSUAM §8035.100, *Information Security Awareness and Training*, states that each campus must implement a program for providing appropriate information security awareness and training to employees appropriate to their access to campus information assets. The campus information security awareness program must promote campus strategies for protecting information assets containing protected data. All employees with access to protected data and information assets must participate in appropriate information security awareness training. When appropriate, information security training must be provided to individuals whose job functions require specialized skill or knowledge in information security.

The CPR CFO stated that CPR did not have an information security awareness training program and had just become aware of such a program available through CSUS.

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 25

We recommend that CPR 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. By December 31, 2011, CPR will work with the campus information security officer to develop and implement an action plan for providing information security awareness training to all employees with access to critical systems or protected data.

DISASTER RECOVERY PLAN

CPR had not completed a comprehensive IT DRP.

We found that the CPR IT DRP did not include a business impact assessment to reflect the criticality and order of recovery priority for CPR-supported systems, had not been updated to address the current financial and membership systems, and lacked reference to other critical computing services such as DNS and Active Directory.

ICSUAM §8085, *Business Continuity and Disaster Recovery*, states that an information security program needs to support the maintenance and potential restoration of operations through and after both minor and catastrophic disruptions. Campuses must ensure that their information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users. Each campus must maintain an ongoing program that ensures the continuity of essential functions and operations following a catastrophic event.

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 DRPs.

The CPR CFO stated that the IT DRP had yet to be completed as it is viewed by CPR as part of its full business continuity plan, which is still in progress.

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 26

We recommend that CPR complete a comprehensive IT DRP that includes a business impact assessment to reflect the criticality and order of recovery priority for CPR-supported systems, addresses the current financial and membership systems, and references other critical computing services such as DNS and Active Directory.

Campus Response

We concur. By March 31, 2012, CPR will work with the campus IT disaster recovery coordinator to develop and implement a comprehensive IT DRP that includes a business impact assessment to reflect the criticality and order of recovery priority for CPR-supported systems, addresses the current financial and membership systems, and references other critical computing services such as DNS, identify management, and Active Directory.

**ASSOCIATED STUDENTS OF
CALIFORNIA STATE UNIVERSITY, SACRAMENTO**

OPERATIONAL COMPLIANCE

The Associated Students of California State University, Sacramento (ASI) had not developed written policies and procedures to address the accounting and processing of accounts receivable.

Specifically, we found that policies and procedures had not been developed to address:

- ▶ Aging and collection of past-due accounts receivable.
- ▶ Valuation of allowance for doubtful accounts receivable.

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 development of policies and procedures to address the collection of outstanding accounts receivable.

The ASI director of finance and administration stated that a formal written policy for accounts receivable was in place; however, it did not specifically address past due accounts receivable due to their immateriality.

The absence of written policies and procedures increases the risk that errors, inconsistencies, misunderstandings, or misappropriation of funds will occur.

Recommendation 27

We recommend that ASI develop written policies and procedures to address the bulleted items noted above regarding the accounting and processing of accounts receivable.

Campus Response

We concur. By December 31, 2011, ASI will develop written policies and procedures, which will address the accounting and processing of accounts receivable, specifically, the aging and collection of past-due accounts receivable and the valuation of allowance for doubtful accounts receivable.

SEGREGATION OF DUTIES

Certain duties and responsibilities related to accounts payable processing were not adequately segregated at ASI.

We found that two accounts payable personnel performed the following incompatible duties:

- ▶ Added vendors to the vendor master file.
- ▶ Reviewed expenditures for supporting documentation and proper authorization.
- ▶ Entered data into the accounts payable system to process payments.

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 8.9.5, *Procurement*, states that the auxiliary should establish a written control system that provides purchase orders and service contracts are prepared separately from receiving and shipping, payables and disbursements, and that identifies unallowable transactions, such as with governing board members.

The ASI director of finance and administration stated that vendor entry was performed by the accounting technician due to limited resources.

Inadequate segregation of duties increases the risk that errors and irregularities will not be detected in a timely manner.

Recommendation 28

We recommend that ASI appropriately segregate certain accounts payable processing functions, or institute mitigating procedures approved by the campus CFO.

Campus Response

We concur. By December 31, 2011, ASI will re-evaluate the segregation of certain accounts payable functions. Controls will be established to ensure appropriate segregation of these duties using current personnel.

CASH RECEIPTS AND HANDLING

Checks received at ASI were neither adequately safeguarded nor deposited in a timely manner, and accountability for cash receipts was not always localized to a specific employee.

We found that:

- ▶ Checks were placed unsecured on top of a safe in the ASI cashiering office during business hours. Routine deposits occurred every Tuesday, and therefore checks were left unsecured for up to one week.

- ▶ Separate opening and close-out procedures were not used to establish accountability when multiple cashiers used the same cash register.

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 adequate administration of cash receipts.

The ASI director of finance and administration stated that the checks were placed on the rolling safe, which was located within the cashiering office. He further stated his belief that the checks were properly safeguarded because access to the cashiering office was limited to employees and the rolling safe was secured in the vault at the end of the day. In addition, he stated that the opening and closeout procedures associated with not switching cashiers in the middle of the day had not been implemented due to the scheduling of part-time student cashiers and the time constraints involved with the process.

Inadequate safeguarding and administration of cash receipts increases the risk of loss or misappropriation of funds.

Recommendation 29

We recommend that ASI:

- a. Ensure that all incoming checks are adequately safeguarded upon receipt and deposited in a timely manner.
- b. Localize accountability over receipts when multiple employees operate the same register, or institute mitigating procedures approved by the campus CFO.

Campus Response

We concur.

- a. By December 31, 2011, ASI will develop and implement procedures to ensure that all incoming checks are adequately safeguarded upon receipt and deposited in a timely manner. ASI will lock all checks received in the lock box and will move the box into the large walk-in safe at night for processing the next day. Additionally, ASI will scan all checks by no later than the following business day after receipt.

- b. By December 31, 2011, ASI will implement, as a mitigating control, a mid-day cash count conducted by the student services representative and reviewed by the operations assistant.

FEES, REVENUES, AND RECEIVABLES

Management review of ASI accounts receivable reconciliations was not documented.

We found that management review of accounts receivable monthly reconciliations was not documented for October, November, and December 2010.

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. The compilation further states that the auxiliary should reconcile accounts on a timely basis with independent management review.

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 documentation of timely preparation and independent review of account reconciliations.

The ASI director of finance and administration stated that all accounts receivable reconciliations were completed and reviewed online by accounting staff and the accounting manager, but there was no documentation that a review had taken place because no hard copy reports existed.

Failure to sufficiently document account reconciliations increases the risk that errors and irregularities will not be detected in a timely manner and accountability will not be maintained.

Recommendation 30

We recommend that ASI document managerial review of the accounts receivable monthly reconciliations.

Campus Response

We concur. By September 30, 2011, ASI will record the proper sign-off of accounts receivable monthly reconciliations by business department management.

PERSONNEL AND PAYROLL

ASI employee timesheets were not always approved prior to payroll processing.

We found that the ASI payroll system permitted timesheets to be paid without specific management approval and did not have the capability to generate a report of unapproved timesheets to enable management review prior to the processing of payroll checks.

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 documentation of timely preparation and independent review of account reconciliations.

The ASI director of finance and administration stated that due to the limitations of the Genesis time keeping program, unapproved timesheets were allowed to be imported before the review process by the accounting staff occurred.

Failure to perform a consistent and timely review of payroll-related data increases the risk of inappropriate payroll payments to employees.

Recommendation 31

We recommend that ASI approve all employee timesheets prior to payroll processing.

Campus Response

We concur. By September 30, 2011, ASI will use an Unapproved Time Card report, which all managers must approve and sign to verify that all non-approved listings are approved for payment.

PROPERTY AND EQUIPMENT

Administration of ASI property and equipment needed improvement.

We found that:

- ▶ ASI had not performed an independent physical inventory of all property and equipment. Inventory custodians were asked to confirm the property and equipment in their custody, but there was no independent verification of the confirmations provided by the custodians.
- ▶ Review of monthly reconciliations of the property sub-ledger to the general ledger was not documented.

- ▶ ASI had not consistently tagged property and equipment items.

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 physical inspection of property and equipment on a service life schedule, reconciliation to the general ledger on a timely basis with review by management, and the proper 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 over property and equipment.

The ASI director of finance and administration stated that the verification of the fixed asset inventory was performed on a random sampling of selected assets and not on the complete physical inventory. In addition, he stated that all reconciliations and reviews by ASI accounting staff and the accounting manager were completed and reviewed online. He further stated that inventory of ASI property and equipment had been properly maintained, but due to competing budgetary priorities and resource constraints, asset tagging had not been accomplished.

Insufficient administration of property and equipment increases the risk that property may be lost or stolen or misrepresented in the financial statements.

Recommendation 32

We recommend that ASI:

- a. Perform an independent physical inventory of property and equipment.
- b. Document the monthly reconciliations of the property sub-ledger to the general ledger.
- c. Ensure that all property and equipment is tagged.

Campus Response

We concur. ASI will complete the following:

- a. By September 30, 2011, the ASI business department will complete inventory counts on all assets at all ASI departments. The inventory counts will be completed by individuals who are not the inventory custodians.
- b. By September 30, 2011, ASI will perform and document monthly fixed asset reconciliations.

- c. By December 31, 2011, ASI will tag all new inventory and any current untagged inventory that is identified as theft sensitive property (highly desirable and/or portable).

INFORMATION TECHNOLOGY

Password controls and data security were not always adequate for ASI systems.

We found that:

- ▶ Password security parameters were inadequate for the child care, accounting, payroll, and human resources systems, as there was no minimum password length, password expiration, or automatic sign-off of users after a period of no use, nor were there complexity requirements or restrictions for reuse of passwords or access after repeated failed attempts. This is a repeat finding from the prior Auxiliary Organizations audit.
- ▶ Protected and/or sensitive data was not encrypted when stored in the accounting, payroll, and human resources systems.

CSUS *Supplemental Security Policy for Access Control*, Policy Number: 8060.0 Revised: August 15, 2010, states that adequate password management is a critical aspect of access control. All campus password management is carried out under the authority of the Information Security Officer. All passwords must have a minimum length of any 15 U.S. keyboard characters, with the passphrase being the preferred method for achieving this length. Those having elevated access to confidential information (e.g., access control administrators, systems administrators, etc.) are encouraged to use longer passphrases. All SacLink passwords must also be changed at least annually; passwords with elevated access and privileges to the campus fiscal system must be changed every 120 days, managed using the official campus password management system found at password.csus.edu.

ICSUAM §8045.100, *Information Technology Security*, states that campuses must develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. Each campus must take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

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 and encryption of any protected/sensitive data residing on auxiliary systems.

The ASI IT manager stated that he was unaware that password security parameters and encryption solutions were available for these systems as several different versions had been utilized in recent years.

Inadequate password and login parameters may compromise the authentication credentials of user account privileges that are embedded into applications and operating systems, which in turn may increase the risk of unauthorized access to auxiliary systems and confidential data. 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 33

We recommend that ASI:

- a. Set effective password and login security parameters for the child care, accounting, payroll, and human resources system, in accordance with campus password guidelines, or institute mitigating controls approved by the campus CFO.
- b. Apply encryption controls to the accounting, payroll, and human resources systems and all other ASI systems, computers, databases, and file servers that house protected and/or sensitive data.

Campus Response

We concur.

- a. By December 31, 2011, ASI will work with the campus information security officer to implement applicable campus standards for password and login security for ASI systems. ASI will complete the following to ensure compliance with campus standards for password and login security:
 - Issue a policy relative to passwords and login security parameters applicable to all ASI systems (child care, accounting, payroll, and human resources). At a minimum, this policy will require complex passwords, require that passwords be changed annually, and also provide the procedures related to changing passwords.
 - Set user and password for each EZcare user at the Children's Center, and provide documentation and configuration of users for audit verification.
 - Configure the firewall on ASI3 to only allow access to Abra and MIP through Citrix.
 - Configure local access via VPN, as backup access for MIP.
- b. By December 31, 2011, ASI will apply applicable encryption controls, or other mitigating controls, to the human resources system (Abra) via SQL, and will apply encryption controls, or other mitigating controls, to the accounting and payroll systems (MIP) via the encryption option provided through the application.

UNIVERSITY UNION OPERATION OF
CALIFORNIA STATE UNIVERSITY, SACRAMENTO

OPERATING AND ADMINISTRATIVE AGREEMENTS

The University Union Operation of California State University, Sacramento (Union) performed a function not authorized by its operating agreement with the CSU Trustees, specifically, the administration of stipends.

We found that the Union had paid stipends totaling \$16,758 to a graduate student working in recreational sports and had not reported the stipends to the campus financial aid office.

Title 5 §42502 states that the operating agreement should specify the function or functions that the organization is to manage, operate, or administer.

Title 5 §42500(d) states that a record of financial assistance, such as student loans, scholarships, stipends, and grants-in-aid, shall be forwarded on a timely basis to the campus financial aid office and shall be documented on student financial aid recipient records in that office.

The Union executive director stated that the graduate student was inherited when campus recreation moved from stateside to the auxiliary side, and the need to update the operating agreement was not considered. She further stated that the failure to include stipend administration in the operating agreement and the failure to report stipends to the financial aid office was due to lack of awareness of the compliance requirements.

Failure to include all functions administered by the auxiliary in the operating agreement increases the risk of misunderstandings and miscommunication regarding rights and responsibilities, and the failure to report student stipends to the campus financial aid office may result in an overpayment of financial aid funds and increases the risk of fines and penalties.

Recommendation 34

We recommend that the Union amend its operating agreement to include the administration of scholarship and stipend payments as an authorized function and report all student stipends to the campus financial aid office.

Campus Response

We concur. By September 30, 2011, the Union will amend its operating agreement to include the administration of scholarship and stipend payments as an authorized function. Additionally, the Union will implement procedures to ensure that all student stipends are reported to the campus financial aid office.

PURCHASING AND ACCOUNTS PAYABLE

The Union did not recover a refundable deposit paid in advance for a Union-sponsored trip. We reviewed 10 travel-related disbursements and found that one disbursement included a \$500 refundable deposit that was not recovered by the Union subsequent to the close of the trip on June 7, 2009.

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 disburse cash in a consistent manner utilizing systems that ensure integrity of existing controls, with annual management review.

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 all refundable deposits be monitored for proper recovery.

The Union executive director stated that the deposit was not listed on the year-end accruals as outstanding due to oversight, and therefore, the deposit was not followed up for recovery.

Failure to sufficiently monitor deposits increases the risk of errors, irregularities, and misappropriation of funds.

Recommendation 35

We recommend that the Union recover refundable deposits paid in advance for Union-sponsored trips.

Campus Response

We concur. As of March 10, 2011, the Union submitted a demand letter to the vendor requesting return of the \$500 refundable deposit; however, the Union does not anticipate recovery of those funds. As of June 2011, the Union revised the policies and procedures regarding the tracking of future deposits on rentals and other purchases, and recovery of those deposits, if applicable.

PROPERTY AND EQUIPMENT

Administration of Union property and equipment did not provide for completion of the physical inventory in a timely manner, timely recording of additions and disposals to fixed asset records, timely recording of related depreciation expense to the general ledger, and timely reconciliation of fixed assets accounts to the general ledger.

We found that:

- ▶ The Union had not performed a physical inventory of one-third of its assets for the fiscal year ended June 30, 2010, in accordance with its policy.
- ▶ Property and equipment additions and disposals were only recorded to fixed asset records once annually instead of at the time of receipt/disposition or at least quarterly.
- ▶ Depreciation expense related to newly purchased items was recorded to the general ledger at the end of the fiscal year instead of at least quarterly.
- ▶ The sub-ledger (fixed assets module) was reconciled to the general ledger once annually instead of at least quarterly.

The Union *Property Management Policy* states that not less than one-third of the Union property inventory will be verified yearly during the last month of the fiscal year and this verification shall additionally include all large quantity or especially large dollar items.

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. It further states that the auxiliary should reconcile physical inventories to the general ledger on a timely basis with review by management.

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 Union executive director stated that the 2009/10 physical inventory was not performed due to oversight. She further stated her belief that the Union was in compliance with CSU policies and that and the Union's external auditors had determined that annual reconciliations were satisfactory based on the volume of property transactions.

Insufficient administration of property and equipment increases the risk that property may be lost or stolen or misrepresented in the financial statements.

Recommendation 36

We recommend that the Union:

- a. Perform a periodic, independent physical inventory of its property and equipment in accordance with its policy.
- b. Record property and equipment additions and disposals to the fixed assets records at the time of receipt/disposal, or at least quarterly.
- c. Record depreciation expense to the general ledger at least quarterly.
- d. Reconcile the fixed assets sub-ledger to the general ledger at least quarterly.

Campus Response

We concur. As of June 30, 2011, the Union completed the following:

- a. The Union completed a full independent physical inventory of its property and equipment in accordance with its policy.
- b. The Union updated its assets with all additions and deletions. The Union will record additions and disposals to the fixed asset records quarterly in future fiscal years. The Property Management policy has been updated to reflect this change.
- c. The Union recorded the depreciation expense for the fiscal year 2010/11. The Union will record depreciation expense to the general ledger quarterly in future fiscal years. The Property Management policy has been updated to reflect this change.
- d. The Union reconciled the fixed assets sub-ledger to the general ledger. The Union will reconcile the fixed assets sub-ledger to the general ledger quarterly in future fiscal years. The Property Management policy has been updated to reflect this change.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
CAMPUS	
Alexander Gonzalez	President
Adam Cook	Information Security Analyst
Larry Gilbert	Vice President and Chief Information Officer
Carole Hayashino	Vice President, University Advancement
Yavette Hayward	Senior Management Auditor
Justine Heartt	Associate Vice President for Financial Services
Ted Koubiar	Director of Operations and System Services
Mike Lee	Vice President for Administration and Chief Financial Officer
Kathi McCoy	Director, Auditing Services
Jason Musselman	Networking Security Analyst
Helen Norris	Associate Vice President for Administrative Computing
Vince Sales	Associate Vice President for Development
Jeff Williams	Information Security Officer
Russell Wyatt	Finance Systems Lead

THE UNIVERSITY FOUNDATION AT SACRAMENTO STATE

Sue Garcia	Director, Advancement Services
Carole Hayashino	Corporate Secretary and Vice President of Advancement
John Koch	Director, Planned Giving
Marisa Rollin	Financial Gift Steward
Vince Sales	Board of Director and Associate Vice President, Development

UNIVERSITY ENTERPRISES, INC.

Vinicio Arriola	Manager, Courtyard Market, Dining Services
Desiree Baker	Retail Manager, Dining Services
Craig Barth	Chief Financial Officer
Stacy Bounds	Cash Room Supervisor
Emily Chu	Controller
Rudolf Egger	Director, Dining Services
Dennis Howes	Supervisor, Dining Services
Nicole Johnson	Dining Services Clerk
Monica Kauppinen	Director, Contract and Research Administration
Trina Knight	Director, Human Resources
Terry Kuntz	Purchasing Manager, Dining Services
Ada Lai	Business Analyst
Mark Lewandowski	Assistant Director, Dining Services
Meri McGraw	Director, Information Technology
Donna McLeod	Payroll Manager
Veronica Nute	Assistant Director, Administration and Operations
Briggett Reilly	Director, Property Services
Jim Reinhart	Executive Director
Lisa Rogers	Assistant Director, Campus Catering

UNIVERSITY ENTERPRISES, INC. (CONT.)

Mery Ali Sastra	Dining Services Coordinator
Sandy Siu	Accounting/Budget Manager
Cathy Sorace	Accounts Receivable Supervisor
Cheryl Stone	Accounts Payable Supervisor

CAPITAL PUBLIC RADIO, INC.

Rick Copeland	Information Technology Coordinator
Barbara Dolder	Director, Member Services
Susan Damberger	Executive Assistant
Rick Eytcheson	President and General Manager
Arla Gibson	Director, Development and Marketing
Victoria Hagele	Business Operations Officer
Jennifer Halm	Member Communications Manager
Jun Reina	Chief Financial Officer

**ASSOCIATED STUDENTS OF
CALIFORNIA STATE UNIVERSITY, SACRAMENTO**

David Brown	Director, Student Life and Services
Brian Dulgar	Director, Aquatic Center
Tatyana Dyda	Accounting Technician
Elvia Felix	Accounting Technician
Jeri Krajewski	Accounting Manager
Michael Lopez-Garcia	Operations Assistant
Stacy Matthews	Lead Payroll Technician
Mark Montalvo	Director, Finance and Administration
Leah Railey	Director, Human Resources
Mari Ruiz	Operations Supervisor
Alicia Taylor	Programs Specialist, Peak Adventures
Gerald Tubo	Information Technology Manager
Denise Wessels	Director, Children's Center
Pat Worley	Executive Director
Jael Young	Director, Peak Adventures

**UNIVERSITY UNION OPERATION OF
CALIFORNIA STATE UNIVERSITY, SACRAMENTO**

Teresa Carle	Accounting Technician
Leslie Davis	Executive Director
Jill Farrell	Business Manager
Steve Forseth	Manager, Custodial Services
Mary Lyons	Union Secretary
Bill Olmsted	Director, Union
Norma Sanchez	Manager, Public Information and Leisure Services
Andrew Singletary	Information Technology Services Manager
Dean Sorensen	Director, Collaborative Services

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, Sacramento
Office of the Vice President & Chief Financial Officer
6000 J Street • Sacramento Hall 272 • Sacramento, CA 95819-6038
T (916) 278-6312 • F (916) 278-5783 • www.csus.edu/aba

September 15, 2011

RECEIVED
UNIVERSITY AUDITOR

SEP 15 2011

THE CALIFORNIA STATE
UNIVERSITY

Larry Mandel
University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802-4210

SUBJECT: Campus Response to Recommendations
of Auxiliary Organization Audit, Report #11-01

Dear Mr. Mandel: *Larry*

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

If you have any questions or require additional information, please contact Kathi McCoy, Director of Auditing Services, at 916 278-7439.

Sincerely,

Ming-Tung

Ming-Tung "Mike" Lee, Ph.D.
Vice President & Chief Financial Officer

MTL:kd

Enclosure

- cc: Alexander Gonzalez, President
- Larry Gilbert, Vice President and Chief Information Officer
- Carole Hayashino, Vice President for University Advancement
- Leslie Davis, Executive Director, University Union Operation
- Rick Eytcheson, President & General Manager, Capital Public Radio, Inc.
- Jim Reinhart, Executive Director, University Enterprises, Inc.
- Patricia Worley, Executive Director, Associated Students, Inc.
- Justine Heartt, Associate Vice President for Financial Services
- Abbi Stone, Associate Vice President for Business & Administrative Services
- Kathi McCoy, Director, Auditing Services

AUXILIARY ORGANIZATIONS
CALIFORNIA STATE UNIVERSITY,
SACRAMENTO

Audit Report 11-01

CAMPUS

FISCAL COMPLIANCE

Recommendation 1

We recommend that the campus require full reimbursement by the auxiliaries for indirect costs incurred by the campus for public safety and IRT support services provided to the auxiliaries.

Campus Response

We concur. As of the 2011/12 fiscal year, the campus will require full reimbursement by the auxiliaries for indirect costs incurred by the campus for public safety and IRT support services provided to the auxiliaries. By October 31, 2011, cost allocation memos and invoices will be distributed to the auxiliary organizations.

CAMPUS OVERSIGHT AND CONTROL

Recommendation 2

We recommend that the campus evaluate the relationship between CPR and the other nonprofit organizations to ensure that the current structure is appropriate and authorized by the CSU and campus and to identify and address potential risks associated with the relationships.

Campus Response

✓ We concur. During August 2011, the campus created a CPR task force, whose mission is to develop recommendations for the president associated with the appropriate placement of CPR Endowment and Tower 91 in relationship with the University and CPR. Based on those results, the campus will implement the appropriate organizational structure, and develop the necessary documentation and agreements.

The recommendations of the CPR task force will be submitted to the campus president by January 31, 2012. Task force membership consists of CPR president & general manager, CPR CFO, Chair of CPR Board of Directors, vice president for university advancement, associate vice president for business & administrative services, and campus auditor.

INFORMATION TECHNOLOGY

PASSWORD SECURITY

Recommendation 3

We recommend that the campus set password security parameters for the donor systems in accordance with campus policy and perform an assessment of password security parameters for all other campus systems used by auxiliary organizations.

Campus Response

We concur. By December 31, 2011, the campus will integrate the donor systems into established campus-wide controls. Additionally, the campus will perform and document an assessment of password security parameters for all other campus systems used by auxiliary organizations, and implement appropriate password controls.

DISASTER RECOVERY PLAN

Recommendation 4

We recommend that the campus update the IT DRP to include adequate details for the recovery of the donor systems.

Campus Response

We concur. By December 31, 2011, the campus will update the IT DRP to include adequate details regarding the expectation for recovery of the donor systems, consistent with the recovery expectations for other non-mission critical systems.

THE UNIVERSITY FOUNDATION AT SACRAMENTO STATE

OPERATIONAL COMPLIANCE

RISK MANAGEMENT

Recommendation 5

We recommend that the Foundation develop and adopt a comprehensive written risk management policy that includes procedures to actively identify, analyze, quantify, and manage risk.

Campus Response

We concur. By December 31, 2011, the Foundation will develop and adopt a comprehensive written risk management policy that includes procedures to actively identify, analyze, quantify, and manage risk.

CONFLICT OF INTEREST

Recommendation 6

We recommend that the Foundation obtain annual conflict of interest statements from all board members.

Campus Response

We concur. As of June 2011, the Foundation Board obtained the conflict of interest statements from all members serving during 2011/12.

UNIVERSITY ENTERPRISES, INC.

OPERATING AND ADMINISTRATIVE AGREEMENTS

Recommendation 7

We recommend that UEI:

- a. Amend the cited agreements with appropriate indemnification and right to audit provisions.
- b. Ensure all future agreements include appropriate indemnification and right to audit provisions.

Campus Response

We concur. UEI will revise the cited agreements to include the appropriate indemnification and right to audit provisions. Additionally, UEI will revise its lease and sub-award agreement templates to contain the appropriate indemnification and right to audit provisions. These actions will be completed by September 30, 2011.

FEES, REVENUES, AND RECEIVABLES

Recommendation 8

We recommend that UEI:

- a. Develop written policies and procedures to periodically audit the sales revenues of the outsourced food and dining services to verify the accuracy of sales commission paid to UEI.
- b. Complete sales audits in a timely manner.
- c. Ensure that sales audits are completed by an independent person.

Campus Response

We concur. Effective June 2011, the following was implemented:

- a. UEI developed and implemented a written policy, *Dining Services/Business Services Vendors' Sales and Commission Audit*, and procedures for the performance of periodic audits of the sales revenues of the outsourced food and dining services to verify the accuracy of sales commissions paid to UEI. A component of these procedures includes the completion and review of a spreadsheet listing the vendors and dates of sale revenue audits, along with the results of audits completed.
- b. A regular, rotating audit schedule was created to include five randomly selected vendors to be audited each fiscal year, with those audits covering a two month period. The timing of the audits is such that each vendor is guaranteed to be audited no less than once every two years. UEI's controller will review the spreadsheet calendar to ensure that all audits are completed by the prescribed dates.

- c. The completion of the sales audits was assigned to the accounts receivable department under the supervision of the controller, both independent parties, with assistance provided as necessary by dining services personnel.

AUXILIARY PROGRAMS

Recommendation 9

We recommend that UEI request faculty members' campus work assignments for inclusion in its calculation of the actual level of faculty effort provided to sponsored projects.

Campus Response

We concur. By March 31, 2012, RACA will develop and implement a procedure with relevant campus units to obtain and assess a copy of the faculty workload report for each new award. Copies of the workload report will be maintained on file.

INFORMATION TECHNOLOGY

DATA SECURITY AND ASSESSMENT

Recommendation 10

We recommend that UEI:

- a. Apply encryption controls to the financial and payroll systems and all other UEI systems, computers, databases, and file servers that house protected and/or sensitive data, or institute mitigating controls approved by the campus chief financial officer (CFO).
- b. Perform an assessment of protected information residing on the administrative file server.

Campus Response

- a. We concur. By December 31, 2011, UEI will apply applicable encryption or other mitigating controls to the financial and payroll systems and all other UEI systems, computers, databases, and file servers that house protected and/or sensitive data.
- b. We concur. As of July 2011, UEI conducted an assessment of each departmental drive, and assessments of all data storage will be performed on an annual basis.

NETWORK SECURITY

Recommendation 11

We recommend that UEI place Internet-accessible web servers on a separate network segment from other production servers.

Campus Response

We concur. By December 31, 2011, UEI will work with campus IRT to appropriately segment public facing servers on the network.

DOMAIN ADMINISTRATION**Recommendation 12**

We recommend that UEI house all user accounts in the unified Active Directory domain or obtain written exception from the campus.

Campus Response

We concur. UEI requested an exception to this security policy from the campus. This exception request is under review by the campus, and a determination will be made by December 31, 2011.

SYSTEM BACKUPS**Recommendation 13**

We recommend that UEI store backups at an off-site location.

Campus Response

We concur. As of March 2011, UEI tapes have been stored off-site on a weekly rotation via Access Information Management.

DISASTER RECOVERY PLAN**Recommendation 14**

We recommend that UEI update its IT DRP to include reference to the CBORD, Active Directory, and email systems.

Campus Response

We concur. By January 31, 2012, UEI will update Disaster Recovery documentation to include references to the CBORD, Active Directory, and email systems.

UNIVERSITY ENTERPRISES DEVELOPMENT GROUP

FACILITIES AGREEMENTS

Recommendation 15

We recommend that UEDG:

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

Campus Response

We concur. As of July 2011, UEI, the assignee of UEDG's agreements, obtained a signed lease amendment from the food operator reflecting the corrected indemnification provisions. As of August 2011, UEI submitted an amendment with corrected indemnification provisions to the fitness center for their signature, with the expectation that the signed amendment will be received by December 31, 2011. The lease template used for all third party leases was revised as of July 2011, and contains the correct indemnification provisions.

CAPITAL PUBLIC RADIO, INC.**OPERATING AND ADMINISTRATIVE AGREEMENTS****Recommendation 16**

We recommend that CPR:

- a. Amend its operating agreement to include an essential function of CSU auxiliary organizations determined/authorized by the CSU Board of Trustees.
- b. Provide instructionally related activities for the benefit of CSUS students.
- c. Decline payments from the university for service orders that are required to be performed without remuneration by its operating agreement with the university.

Campus Response

We concur. The campus and CPR will amend the CPR operating agreement to properly substantiate its essential function as a CSU auxiliary organization. The campus and CPR will provide relevant instructionally-related activities for the benefit of Sacramento State students.

During August 2011, the campus created a CPR task force, whose mission is to develop recommendations for the president regarding revisions to the CPR operating agreement, in particular that the operating agreement will include an essential function of CSU auxiliary organizations as determined and authorized by the CSU Board of Trustees. Additionally, the task force will define instructionally-related activities, and provide guidance regarding the implementation of instructionally-related activities accessible to our students, and associated with the operation of CPR.

The recommendations of the CPR task force will be submitted to the campus president by January 31, 2012. Task force membership consists of CPR president & general manager, CPR CFO, Chair of CPR Board of Directors, vice president for university advancement, associate vice president for business & administrative services, and campus auditor.

Since 2008/09, CPR has not accepted any payments from the university related to service orders that are required to be performed without remuneration by its operating agreement with the university. Additionally, CPR will not accept any payments of this nature in the future.

OPERATIONAL COMPLIANCE**Recommendation 17**

We recommend that CPR develop and adopt a comprehensive written risk management policy, including procedures to actively identify, analyze, quantify, and manage risk.

Campus Response

We concur. By December 31, 2011, CPR will develop and adopt a comprehensive written risk management policy that includes procedures to actively identify, analyze, quantify, and manage risk.

FEES, REVENUES, AND RECEIVABLES

ACCOUNTS RECEIVABLE

Recommendation 18

We recommend that CPR:

- a. Promptly pursue the collection of delinquent pledges receivable.
- b. Document managerial review of the pledges receivable aging report.
- c. Write off long outstanding pledges receivable in a timely manner.
- d. Document policies and procedures for the monitoring of pledges receivable, collection of delinquent pledges, and write-off of uncollectible pledges.

Campus Response

We concur. By December 31, 2011, CPR will complete the following:

- a. CPR will develop and implement procedures to promptly pursue the collection of delinquent pledges receivable.
- b. CPR will develop and implement procedures related to the required documentation of the managerial review of the pledges receivable aging report.
- c. CPR will develop and implement procedures related to the write off of long outstanding pledges receivable in a timely manner.
- d. CPR will develop and implement policies and procedures for the monitoring of pledges receivable, collection of delinquent pledges, and write-off of uncollectible pledges.

MATCHING GIFTS

Recommendation 19

We recommend that CPR:

- a. Maintain documentation of matching gift dual review in support of the evaluation and receipt of corporate matching gifts to ensure that funds are administered in accordance with corporate donor requirements and deposited as directed in a timely manner.
- b. Manually correct/write-off auto-added pledges, disable the auto-added feature within the database, and ensure that pledges are entered at the constituents' requests.
- c. Follow-up and/or write-off aged outstanding matching gifts.

Campus Response

We concur. By December 31, 2011, CPR will improve the administration of corporate matching gifts:

- a. CPR will develop and implement procedures related to corporate matching gifts. At a minimum, these procedures will address the retention of documentation to evidence that gifts were evaluated for eligibility of matching, were subjected to a dual review to ensure that funds were administered in accordance with corporate donor requirements, were deposited as directed and in a timely manner, and ensure that only pledges based on constituents' requests are entered to the database.
- b. CPR will write-off the auto-added pledges, and will disable the auto-added feature within the database. Based on newly implemented procedures, CPR will ensure that pledges are entered based on the constituents' requests.
- c. CPR will write-off outstanding matching gifts that are more than 12 months past due or had no donor-directed activity within the past 12 months. The write-off information will be noted in the donor's account, using Raiser's Edge.

INFORMATION TECHNOLOGY**PAYMENT CARD INDUSTRY DATA SECURITY STANDARD COMPLIANCE****Recommendation 20**

We recommend that CPR:

- a. Redact and adequately secure credit card information when not in use, or discard the information immediately after successful processing.
- b. Ensure PCI DSS-compliant configuration on the CPR firewall that protects the workstations used to enter credit card data into the Raiser's Edge online system.

Campus Response

We concur. By December 31, 2011, CPR will complete the following:

- a. CPR will work with the campus information security officer to complete a full assessment and analysis of CPR's compliance with the latest PCI standards. Based on the results of that assessment and analysis, CPR will develop and implement procedures required by those PCI standards applicable to the campus, and the procedures will include when to redact and secure credit card information when not in use and when to discard the information immediately after successful processing.
- b. CPR will work with campus IRT to develop and implement a PCI DSS-compliant configuration on the campus firewalls and CPR workstations and systems used to enter and process credit card data into the Raiser's Edge online system.

PASSWORD AND DATA SECURITY

Recommendation 21

We recommend that CPR:

- a. Set effective password and login security parameters for the Sage Business Works accounting system in accordance with campus password guidelines, or institute mitigating controls approved by the campus CFO.
- b. Apply encryption controls to the accounting and donor systems and all other CPR systems, computers, databases, and file servers that house protected and/or sensitive data.

Campus Response

We concur. By December 31, 2011, CPR will complete the following:

- a. CPR will work with the campus information security officer to set and implement applicable campus standards for password and login security for Sage Business Works.
- b. CPR will apply applicable encryption or other mitigating controls to the accounting and donor systems and all other CPR or campus systems, computers, databases, and file servers that house and process protected and/or sensitive data. CPR will work with the campus information security officer to complete an assessment and analysis of servers handling sensitive data, to determine if those servers should be housed in the secure campus data center.

USER ACCESS REVIEW

Recommendation 22

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

Campus Response

We concur. By December 31, 2011, CPR will work with campus IRT to develop and implement policies and procedures regarding the documented management reviews of user access privileges for all critical systems and applications containing protected data. The user access review will be conducted on an annual basis. These policies and procedures will be in compliance with campus policies and procedures.

DOMAIN ADMINISTRATION

Recommendation 23

We recommend that CPR house all user accounts in the unified Active Directory domain or apply for written exception from the campus, in accordance with campus policy.

Campus Response

We concur. By December 31, 2011, CPR will work with the campus information security officer to maintain all user accounts in the campus unified active directory domain.

NETWORK ADMINISTRATION**Recommendation 24**

We recommend that CPR ensure that all network infrastructure devices are registered with the campus information security officer and specifically authorized for use as part of the campus network infrastructure, or apply for written exception from the campus information security officer for the operation of an independent network.

Campus Response

We concur. By December 31, 2011, CPR will work with campus IRT to register all network devices, to ensure compliance with all campus infrastructure security policies, and to apply for a written exception to operate applicable independent network segments.

INFORMATION SECURITY AWARENESS TRAINING**Recommendation 25**

We recommend that CPR 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. By December 31, 2011, CPR will work with the campus information security officer to develop and implement an action plan for providing information security awareness training to all employees with access to critical systems or protected data.

DISASTER RECOVERY PLAN**Recommendation 26**

We recommend that CPR complete a comprehensive IT DRP that includes a business impact assessment to reflect the criticality and order of recovery priority for CPR-supported systems, addresses the current financial and membership systems, and references other critical computing services such as DNS and Active Directory.

Campus Response

We concur. By March 31, 2012, CPR will work with the campus IT disaster recovery coordinator to develop and implement a comprehensive IT DRP that includes a business impact assessment to reflect the criticality and order of recovery priority for CPR-supported systems, addresses the current financial and membership systems, and references other critical computing services such as DNS, identify management, and Active Directory.

**ASSOCIATED STUDENTS OF
CALIFORNIA STATE UNIVERSITY, SACRAMENTO**

OPERATIONAL COMPLIANCE

Recommendation 27

We recommend that ASI develop written policies and procedures to address the bulleted items noted above regarding the accounting and processing of accounts receivable.

Campus Response

We concur. By December 31, 2011, ASI will develop written policies and procedures, which will address the accounting and processing of accounts receivable, specifically, the aging and collection of past due accounts receivable and the valuation of allowance for doubtful accounts receivable.

SEGREGATION OF DUTIES

Recommendation 28

We recommend that ASI appropriately segregate certain accounts payable processing functions, or institute mitigating procedures approved by the campus CFO.

Campus Response

We concur. By December 31, 2011 ASI will re-evaluate the segregation of certain accounts payable functions. Controls will be established to ensure appropriate segregation of these duties using current personnel.

CASH RECEIPTS AND HANDLING

Recommendation 29

We recommend that ASI:

- a. Ensure that all incoming checks are adequately safeguarded upon receipt and deposited in a timely manner.
- b. Localize accountability over receipts when multiple employees operate the same register, or institute mitigating procedures approved by the campus CFO.

Campus Response

We concur.

- a. By December 31, 2011, ASI will develop and implement procedures to ensure that all incoming checks are adequately safeguarded upon receipt and deposited in a timely manner. ASI will lock all checks received in the lock box and will move the box into the large walk-in safe at night for

processing the next day. Additionally, ASI will scan all checks by no later than the following business day after receipt.

- b. By December 31, 2011, ASI will implement, as a mitigating control, a mid-day cash count conducted by the student services representative and reviewed by the operations assistant.

FEES, REVENUES, AND RECEIVABLES

Recommendation 30

We recommend that ASI document managerial review of the accounts receivable monthly reconciliations.

Campus Response

We concur. By September 30, 2011, ASI will record the proper “sign-off” of accounts receivable monthly reconciliations by business department management.

PERSONNEL AND PAYROLL

Recommendation 31

We recommend that ASI approve all employee timesheets prior to payroll processing.

Campus Response

We concur. By September 30, 2011, ASI will use an “Unapproved Time Card” report, which all managers must approve and sign to verify that all non-approved listings are approved for payment.

PROPERTY AND EQUIPMENT

Recommendation 32

We recommend that ASI:

- a. Perform an independent physical inventory of property and equipment.
- b. Document the monthly reconciliations of the property sub-ledger to the general ledger.
- c. Ensure that all property and equipment is tagged.

Campus Response

We concur. ASI will complete the following:

- a. By September 30, 2011, the ASI business department will complete inventory counts on all assets at all ASI departments. The inventory counts will be completed by individuals who are not the inventory custodians.

- b. By September 30, 2011, ASI will perform and document monthly fixed asset reconciliations.
- c. By December 31, 2011, ASI will tag all new inventory and any current untagged inventory that is identified as “theft sensitive” property (highly desirable and/or portable).

INFORMATION TECHNOLOGY

Recommendation 33

We recommend that ASI:

- a. Set effective password and login security parameters for the child care, accounting, payroll, and human resources system, in accordance with campus password guidelines, or institute mitigating controls approved by the campus CFO.
- b. Apply encryption controls to the accounting, payroll, and human resources systems and all other ASI systems, computers, databases, and file servers that house protected and/or sensitive data.

Campus Response

We concur.

- a. By December 31, 2011, ASI will work with the campus information security officer to implement applicable campus standards for password and login security for ASI systems. ASI will complete the following to ensure compliance with campus standards for password and login security:
 - Issue a policy relative to passwords and login security parameters applicable to all ASI systems (child care, accounting, payroll, and human resources). At a minimum, this policy will require complex passwords, require that passwords be changed annually, and also provide the procedures related to changing passwords.
 - Set user and password for each EZcare user at the Children’s Center, and provide documentation and configuration of users for audit verification.
 - Configure the firewall on ASI3 to only allow access to Abra and MIP through Citrix.
 - Configure local access via VPN, as back up access for MIP.
- b. By December 31, 2011, ASI will apply applicable encryption controls, or other mitigating controls, to the human resources system (Abra) via SQL, and will apply encryption controls, or other mitigating controls, to the accounting and payroll systems (MIP) via the encryption option provided through the application.

**UNIVERSITY UNION OPERATION OF
CALIFORNIA STATE UNIVERSITY, SACRAMENTO**

OPERATING AND ADMINISTRATIVE AGREEMENTS

Recommendation 34

We recommend that the Union amend its operating agreement to include the administration of scholarship and stipend payments as an authorized function and report all student stipends to the campus financial aid office.

Campus Response

We concur. By September 30, 2011, the Union will amend its operating agreement to include the administration of scholarship and stipend payments as an authorized function. Additionally, the Union will implement procedures to ensure that all student stipends are reported to the campus financial aid office.

PURCHASING AND ACCOUNTS PAYABLE

Recommendation 35

We recommend that the Union recover refundable deposits paid in advance for Union-sponsored trips.

Campus Response

We concur. As of March 10, 2011, the Union submitted a demand letter to the vendor requesting return of the \$500 refundable deposit; however, the Union does not anticipate recovery of those funds. As of June 2011, the Union revised the policies and procedures regarding the tracking of future deposits on rentals and other purchases, and recovery of those deposits, if applicable.

PROPERTY AND EQUIPMENT

Recommendation 36

We recommend that the Union:

- a. Perform a periodic, independent physical inventory of its property and equipment in accordance with its policy.
- b. Record property and equipment additions and disposals to the fixed assets records at the time of receipt/disposal, or at least quarterly.
- c. Record depreciation expense to the general ledger at least quarterly.
- d. Reconcile the fixed assets sub-ledger to the general ledger at least quarterly.

Campus Response

We concur. As of June 30, 2011, the Union completed the following:

- a. The Union completed a full independent physical inventory of its property and equipment in accordance with its policy.
- b. The Union updated its assets with all additions and deletions. The Union will record additions and disposals to the fixed asset records quarterly in future fiscal years. The Property Management policy has been updated to reflect this change.
- c. The Union recorded the depreciation expense for the fiscal year 2010/11. The Union will record depreciation expense to the general ledger quarterly in future fiscal years. The Property Management policy has been updated to reflect this change.
- d. The Union reconciled the fixed assets sub-ledger to the general ledger. The Union will reconcile the fixed assets sub-ledger to the general ledger quarterly in future fiscal years. The Property Management policy has been updated to reflect this change.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

CHANNEL ISLANDS

September 27, 2011

CHICO

MEMORANDUM

DOMINGUEZ HILLS

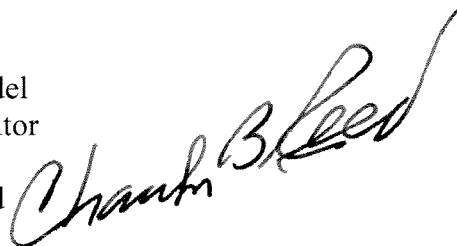
EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FULLERTON

FROM: Charles B. Reed
Chancellor



HUMBOLDT

SUBJECT: Draft Final Report 11-01 on *Auxiliary Organizations*,
California State University, Sacramento

LONG BEACH

LOS ANGELES

In response to your memorandum of September 27, 2011, I accept the response as submitted with the draft final report on *Auxiliary Organizations*, California State University, Sacramento.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS