

**AUXILIARY ORGANIZATIONS**  
**SAN FRANCISCO STATE UNIVERSITY**

**Audit Report 09-17**  
**February 10, 2010**

---

**Members, Committee on Audit**

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

---

**Staff**

University Auditor: Larry Mandel  
Senior Director: Janice Mirza  
Audit Manager: Gary Miller  
Senior Auditors: Dominick Owens and Ken Tsui  
Internal Auditors: Jamar Johnson, Caroline Lee and Salesian Yuen

---

**BOARD OF TRUSTEES**  
**THE CALIFORNIA STATE UNIVERSITY**

---

## **CONTENTS**

Executive Summary .....	1
Introduction.....	6
Background .....	6
Purpose.....	8
Scope and Methodology .....	8

---

## **OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES**

### **CAMPUS**

Operating and Administrative Agreements .....	12
Segregation of Duties.....	13
Property and Equipment .....	14
Information Technology .....	15
Protected Data Assessment.....	15
Payment Card Industry Data Security Standard .....	16
Password Security and User Access .....	18

### **THE UNIVERSITY CORPORATION, SAN FRANCISCO STATE**

Facilities Agreements .....	20
Fiscal Compliance.....	21
Property and Equipment .....	22
Trusts and Other Liabilities .....	23
Endowment Administration.....	25

### **FRANCISCAN SHOPS**

Operating and Administrative Agreements .....	27
Segregation of Duties.....	28
Personnel and Payroll .....	29
Payroll Reconciliation.....	29
Employee Leave.....	30

---

CONTENTS

Information Technology ..... 31  
    Information Security Training and Data Confidentiality Forms ..... 31  
    Password Security ..... 33  
    User Access ..... 34  
    Environmental Controls ..... 35  
    System Backups ..... 36  
    E-mail Systems ..... 38

**ASSOCIATED STUDENTS OF SAN FRANCISCO STATE UNIVERSITY**

Operating and Administrative Agreements ..... 40  
  
Operational Compliance ..... 41  
    Policies and Procedures ..... 41  
    Risk Management ..... 42  
  
Personnel and Payroll ..... 42  
  
Property and Equipment ..... 43

**SAN FRANCISCO STATE UNIVERSITY STUDENT CENTER**

Operational Compliance ..... 45  
  
Petty Cash and Change Funds ..... 46  
  
Personnel and Payroll ..... 47  
    Policies and Procedures ..... 47  
    Payroll Reconciliation ..... 48

## **APPENDICES**

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

---

## **ABBREVIATIONS**

ABS	Auxiliary Business Services
AS	Associated Students of San Francisco State University
CFO	Chief Financial Officer
CFS	Common Financial System
Corporation	The University Corporation, San Francisco State
CSU	California State University
EO	Executive Order
HR	Human Resources
IT	Information Technology
PCI DSS	Payment Card Industry Data Security Standard
RFIN	Resolution of the Committee on Finance
SAQ	Self Assessment Questionnaire
SFSU	San Francisco State University
Shops	Franciscan Shops
Student Center	San Francisco State University Student Center

---

## 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.

San Francisco State University (SFSU) 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 SFSU campus and its auxiliary organizations from July 20, 2009, through August 21, 2009, and made a study and evaluation of the system of internal compliance/internal control in effect as of August 21, 2009. This report represents our triennial review.

Our study and evaluation at *San Francisco State University Foundation* did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. In our opinion, the accounting and administrative control in effect as of August 21, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *The University Corporation, San Francisco State* 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 trusts and other liabilities. 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 August 21, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *Franciscan Shops* 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: payroll and personnel, 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 August 21, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *Associated Students of San Francisco State University* 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: operational compliance, and property and equipment. 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 August 21, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *San Francisco State University Student Center* 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: operational compliance, and payroll and personnel. 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 August 21, 2009, taken as a whole, was sufficient to meet the objectives stated above.

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

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

## **CAMPUS**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS [12]**

A business arrangement between the campus and a third-party vendor was not supported by a complete and/or written agreement.

### **SEGREGATION OF DUTIES [13]**

Certain duties and responsibilities related to payroll and personnel processing provided by auxiliary business services (ABS) to The University Corporation, San Francisco State (Corporation), Associated Students of San Francisco State University (AS), and the San Francisco State University Student Center (Student Center) were not adequately segregated. This is a repeat finding for the Corporation from a prior Auxiliary Organizations audit report.

### **PROPERTY AND EQUIPMENT [14]**

Campus ABS administration of AS and Student Center property and equipment did not provide for timely recording of additions to fixed asset records and related depreciation expense to the general ledger.

### **INFORMATION TECHNOLOGY [15]**

The campus did not ensure that the auxiliaries perform a periodic, detailed assessment and inventory of protected information residing on auxiliary systems and fully address Payment Card Industry Data Security Standard requirements. Further, password and login security and user access were not always adequate for auxiliary systems administered by campus ABS.

## **THE UNIVERSITY CORPORATION, SAN FRANCISCO STATE**

### **FACILITIES AGREEMENTS [20]**

Certain lease and sublease agreements between The University Corporation, San Francisco State (Corporation) and other entities had not been amended to reflect the new name of the auxiliary and/or did not include appropriate indemnification provisions.

### **FISCAL COMPLIANCE [21]**

The Corporation did not record board-designated reserves within the general ledger in accordance with its reserve policy. This is a repeat finding from the prior Auxiliary Organizations audit.

### **PROPERTY AND EQUIPMENT [22]**

Administration of Corporation property and equipment did not provide for timely disposition because property and equipment dispositions were only communicated to the campus ABS unit for removal from the general ledger once annually instead of at the time of disposition.

### **TRUSTS AND OTHER LIABILITIES [23]**

Certain campus program revenues may be inappropriately deposited to, and held in custody by, the Corporation. This is a repeat finding from the prior Auxiliary Organizations audit.

## **ENDOWMENT ADMINISTRATION [25]**

Certain Corporation endowment files lacked executed endowment agreements and/or account set-up forms, and some endowment agreements did not delineate administrative fees.

## **FRANCISCAN SHOPS**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS [27]**

The arrangement between Franciscan Shops (Shops) and a third-party service provider that performed physical inventory counts was not supported by a service agreement that included appropriate insurance and indemnification provisions.

### **SEGREGATION OF DUTIES [28]**

Certain duties and responsibilities related to the processing of human resources and payroll transactions were not adequately segregated at Shops.

### **PERSONNEL AND PAYROLL [29]**

Payroll tax reconciliations were not timely reviewed by Shops management. In addition, employee leave accounting required improvement. Employee vacation and sick leave accounting was recorded and tracked via one Excel spreadsheet maintained locally on one employee's computer, which was not electronically backed up on any periodic basis; and monthly updates to employee vacation and sick leave balances and adjustments to leave accrual rates were not reviewed or reconciled by an independent manager subsequent to the payroll accountant's data entry.

### **INFORMATION TECHNOLOGY [31]**

Shops personnel with access to critical systems or protected data were not required to complete information security awareness training or sign data confidentiality forms. Password and login security controls were not always adequate for Shops systems, and user access to Shops systems was not adequately reviewed or administered. Further, the Shops server room lacked fire or smoke detection devices and was equipped with a problematic fire suppression system for a room storing critical servers/systems. In addition, the Shops process to backup payroll data transmitted to an off-site service provider was neither effective nor adequately secure, e-mail policies and procedures were not documented, and e-mail password security controls were not adequate.

## **ASSOCIATED STUDENTS OF SAN FRANCISCO STATE UNIVERSITY**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS [40]**

Certain agreements between Associated Students of San Francisco State University (AS) and independent contractors did not include appropriate insurance and indemnification provisions.

### **OPERATIONAL COMPLIANCE [41]**

AS had not developed written policies and procedures to address the accounting and processing of accounts receivable, nor had AS developed a written risk management policy.

### **PERSONNEL AND PAYROLL [42]**

AS did not perform a detailed, documented reconciliation of AS-generated payroll reports against the ADP payroll records processed by ABS.

### **PROPERTY AND EQUIPMENT [43]**

Administration of AS property and equipment did not provide for timely disposition because property and equipment dispositions were only communicated to the campus ABS unit for removal from the general ledger once annually instead of at the time of disposition.

## **SAN FRANCISCO STATE UNIVERSITY STUDENT CENTER**

### **OPERATIONAL COMPLIANCE [45]**

The San Francisco State University Student Center (Student Center) had not developed written policies and procedures to fully address the accounting and processing of accounts receivable.

### **PETTY CASH AND CHANGE FUND [46]**

Administration of Student Center change and petty cash funds required improvement. There was no definitive explanation for fund shortages, independent cash counts of change and petty cash funds were only performed on an annual basis, and not all change funds were physically counted during these annual independent cash counts.

### **PERSONNEL AND PAYROLL [47]**

The Student Center did not have written policies or procedures pertaining to the semimonthly payroll process. In addition, the Student Center did not perform a detailed, documented reconciliation of Student Center-generated payroll reports against the ADP payroll records processed by ABS.

---

## 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 San Francisco State University Foundation (Foundation) was established in July 2008 as a non-profit public benefit corporation responsible for developing and increasing the facilities of San Francisco State University (SFSU) for broader educational opportunities and service to students, alumni, and the citizens of California; and providing funding for research and the establishment of scholarships and other student assistance programs, as well as advisory counsel and assistance to the campus president. The Foundation is authorized to receive and process gifts, bequests, endowments, trusts, and other gifts, and to acquire and develop real property. The Foundation will begin operations in October 2009 and acquire all

endowments currently maintained and managed by The University Corporation, San Francisco State beginning July 1, 2010. The Foundation does not have employees and will rely on the university's auxiliary business services (ABS) unit and university advancement personnel for accounting and administrative support services.

The University Corporation, San Francisco State (Corporation) was established in June 2007 and formerly operated under the name of San Francisco State University Foundation, Inc., which was established in 1946 as a non-profit corporation responsible for promoting, assisting, and enhancing the university's educational mission through educational projects, university research and development projects, and community outreach. The Corporation is responsible for the administration of projects and non-federal funds it receives from outside sponsors, as well as the SFSU endowment portfolio. However, the newly formed Foundation will take over the administration of all endowments beginning in fiscal year 2010. As part of its operating agreement with SFSU, the Corporation administers sublease agreements for food and vending services provided by third parties. The Corporation has a limited number of employees and relies on the university's ABS unit for accounting and administrative support services.

Franciscan Shops (Shops) was established in 1982 as a non-profit public benefit corporation. Shops provides a range of retail services either in direct support of the educational mission of the university or as a convenience to the students, faculty, and staff. Shops is responsible for commercial operations, including the bookstore, two convenience stores, and the copy center. The Shops performs all accounting in-house and is governed by a twelve-member board of directors. Funds received are committed to the purposes for which they have been received and are, therefore, unavailable for other activities.

Associated Students of San Francisco State University (AS) was established in 1944 as a non-profit public benefit corporation responsible for providing programs and services integral to the university's educational mission. AS promotes student self-government and provides facilities and programs to satisfy the needs and interests of its members, including a child care center, legal resource center, women's center, and a typing center; an events production program; and other programs that provide various networking, counseling, and mentoring activities. AS also offers graduate and undergraduate scholarships. AS relies on the university's ABS unit for accounting and administrative support services.

The San Francisco State University Student Center (Student Center) was opened on campus in 1975, established as an unincorporated association with 501(c)(3) status in 1976, and then incorporated as a non-profit public benefit corporation in 1996 with the specific and primary purpose of enhancing the educational, social, and cultural development of students, faculty, alumni, and staff of the university. The Student Center serves the student population by providing a myriad of services and programs, including restaurants, meeting rooms, a conference hall, a game room, automated teller machines, transit passes, art exhibits, live bands, and community-based events. In addition, space is leased to AS for administration purposes. Fiscal and administrative functions are shared between the Student Center and the university's ABS unit.

## **PURPOSE**

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

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

## **SCOPE AND METHODOLOGY**

Our study and evaluation were conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors, and included the audit tests we considered necessary in determining that accounting and administrative controls are in place and operative. The management review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor policies, letters, and directives. For those audit tests that required annualized data, fiscal years 2007/08 and 2008/09 were the primary periods reviewed. In certain instances, we were concerned with representations of the most current data; in such cases, the test period was July 1, 2009, to August 21, 2009. Our primary focus was on internal compliance/internal control.

Specifically, we reviewed and tested:

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

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

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

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

San Francisco State University Foundation

- ▶ Operating and Administrative Agreements
- ▶ Corporate Governance
- ▶ Campus Oversight and Control

The University Corporation, San Francisco State

- ▶ 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
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Endowment Administration
- ▶ Auxiliary Programs
- ▶ Information Technology

Franciscan Shops

- ▶ 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

Franciscan Shops (cont.)

- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Information Technology

Associated Students of San Francisco State University

- ▶ 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
- ▶ Personnel and Payroll
- ▶ Property and Equipment

San Francisco State University Student Center

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

Campus (Auxiliary Business Services)

- ▶ Operating and Administrative Agreements
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Information Technology

We have not performed any auditing procedures beyond August 21, 2009. Accordingly, our comments are based on our knowledge as of that date. Since the purpose of our comments is to suggest areas for improvement, comments on favorable matters are not addressed.

---

## **OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES**

### **CAMPUS**

#### **OPERATING AND ADMINISTRATIVE AGREEMENTS**

A business arrangement between the campus and a third-party vendor was not supported by a complete and/or written agreement.

The arrangement between the campus auxiliary business services (ABS) unit and a third-party service provider for payroll services was not supported by a written agreement. The ADP payroll system, which contains protected employee data for The University Corporation, San Francisco State (Corporation), Associated Students of San Francisco State University (AS) and the San Francisco State University Student Center (Student Center) payroll, was hosted off-site by the service provider. The lack of service agreement for this off-site hosting service also resulted in information security and confidentiality terms not being adequately addressed.

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 and incorporate all necessary contractual terms for information security and data confidentiality.

Executive Order (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 California State University (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, arising out of, or in any way connected with the operations of the auxiliary.

The ABS director stated that the campus had utilized the payroll service provider for several years and was unaware of the requirement to document this arrangement within a formal service agreement.

The absence of complete, written agreements increases the risk of misunderstandings and miscommunication regarding rights and responsibilities, while the absence of appropriate information security and confidentiality terms for services involving protected data subjects the auxiliaries and CSU to potential liability.

### **Recommendation 1**

We recommend that the campus establish a written agreement with the payroll service provider; and for all vendor service agreements relating to access to protected records or data, consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities and the confidentiality of data.

### **Campus Response**

We concur. ABS will work with the payroll service provider and incorporate the CSU General Provisions for Information Technology Acquisitions via the purchase order provided to the vendor.

Expected completion date: July 2010

## **SEGREGATION OF DUTIES**

Certain duties and responsibilities related to payroll and personnel processing provided by ABS to the Corporation, AS, and the Student Center were not adequately segregated. This is a repeat finding for the Corporation from a prior Auxiliary Organizations audit report.

We found that four ABS accountants were responsible for performing the following duties for their assigned auxiliaries:

- ▶ Adding or changing personnel records to/in the ADP payroll system.
- ▶ Posting payroll entries to the ADP payroll system.
- ▶ Performing reconciliations of payroll checks paid to ADP payroll system reports.

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 8.9.6, *Payroll*, states that the auxiliary should establish a written controls system that ensures payroll preparation is segregated from the general ledger function and other payroll functions such as hiring authorization, timekeeping, and distribution of checks.

The ABS director stated that duties and responsibilities related to payroll and personnel processing were not properly segregated due to her belief that there were mitigating controls existing outside of the system to prevent problems that could arise when there was one person performing every aspect of a task, such as inputting pay information, setting up new employees, and processing payments. She further stated that all transactions are initiated from the respective auxiliary human resource area by documented and approved forms, the payroll register is forwarded to each respective auxiliary human resource area, and payroll is not distributed by the person processing payroll.

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

### **Recommendation 2**

We recommend that the campus appropriately segregate certain payroll and personnel processing functions or institute mitigating procedures approved by the campus chief financial officer (CFO).

### **Campus Response**

We concur. ABS has taken the appropriate steps to ensure mitigating controls exist outside of the system:

- All input information is initiated by the human resources (HR) function of each auxiliary.
- All new employees created or employee records changed are only initiated with the appropriate documentation. We have implemented a new step to assist in preventing erroneous checks from being created. Before payroll is processed, a change report is produced from the payroll system and reviewed with the supported documentation by the director of ABS or designee.

The approval of the mitigating procedures outlined above will be obtained from the campus CFO.

Expected completion date: June 2010

## **PROPERTY AND EQUIPMENT**

Campus ABS administration of AS and Student Center property and equipment did not provide for timely recording of additions to fixed asset records and related depreciation expense to the general ledger.

We found that:

- ▶ Property and equipment purchases were only recorded to fixed asset records once annually instead of at the time of receipt.
- ▶ Depreciation expense related to newly purchased items was recorded to the general ledger at the end of the fiscal year.

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

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

The ABS director stated that property and equipment additions and related depreciation expense were processed once per year because items purchased throughout the year are reviewed to verify that all assets and leasehold improvements are captured.

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

### **Recommendation 3**

We recommend that the campus record AS and Student Center property and equipment additions when received and record the related depreciation expense on a more frequent basis, at least quarterly.

### **Campus Response**

We concur. ABS has implemented recording additions on a quarterly basis as well as recording the related depreciation expense.

## **INFORMATION TECHNOLOGY**

### **PROTECTED DATA ASSESSMENT**

The campus did not ensure that the auxiliaries perform a periodic, detailed assessment and inventory of protected information residing on auxiliary systems.

The San Francisco State University (SFSU) *Confidentiality and Information Security Plan* establishes appropriate and reasonable administrative, technical, and physical safeguards designed to ensure the security and protection of confidential information in the university's custody, whether in electronic, paper, or other forms.

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

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

allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates periodic assessment and inventory of protected information residing on systems.

The auxiliary executive management stated that they were unaware of the requirement to complete such detailed assessments and inventory of protected information.

Inadequate accountability over information assets, especially those containing critical and/or personal confidential information or with accessibility to such protected information, increases the risk of loss and inappropriate use of auxiliary resources and exposure to information security breaches.

#### **Recommendation 4**

We recommend that the campus ensure that the auxiliaries perform an initial, and then annual, assessment and inventory of protected data on all systems to determine the existence of any protected data and the need for appropriate logical and physical security measures.

#### **Campus Response**

We concur. The campus biennial survey of all campus systems will include auxiliaries.

Expected completion date: July 2010

### **PAYMENT CARD INDUSTRY DATA SECURITY STANDARD**

The campus did not ensure that the auxiliaries had fully addressed Payment Card Industry (PCI) Data Security Standard (DSS) requirements.

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

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

The SFSU *Confidentiality and Information Security Plan* establishes appropriate and reasonable administrative, technical, and physical safeguards designed to ensure the security and protection of confidential information in the university's custody, whether in electronic, paper, or other forms.

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

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

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

The campus information security officer stated that the campus and auxiliaries were aware of PCI DSS requirements but stated that the PCI SAQ and other formal certifications are optional for Level 4 Merchant status (of which both auxiliaries which handle credit cards are). She added that the auxiliary requirements are contractually dictated by their acquirers (acquiring banks and merchant banks).

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

### **Recommendation 5**

We recommend that the campus and auxiliaries:

- a. Define and document roles, responsibilities, and legal determination for PCI DSS compliance between the campus and the auxiliaries.
- b. Conduct and fully document a risk assessment of comprehensive compliance obligations for credit card data maintained on auxiliary servers and transmitted throughout the campus network and stored manually in local files.

- c. Determine whether an annual SAQ is necessary, and if so, then complete an annual SAQ to include all credit card merchants on campus, whether completed jointly or separate from the auxiliaries.

### **Campus Response**

We concur. The campus will request its auxiliary organizations to review their contractual requirements, if appropriate, with their legal counsel, and review segmentation of any electronic transmission which may present liability to the campus.

Expected completion date: July 2010

### **PASSWORD SECURITY AND USER ACCESS**

Password and login security and user access were not always adequate for auxiliary systems administered by campus ABS.

We found that:

- ▶ The password and login security parameters for the ADP payroll system only required a minimum password length of four characters and did not enforce password complexity, periodic expiration, or login security parameters.
- ▶ The password and login security parameters for the child care system did not enforce any minimum password length, password complexity, periodic expiration, or login security. In addition, we found that the passwords for all users were an exact match to the user name which was set as each user's initials (e. g., GDM). Further, one generic user account (i.e., temporary) existed.

SFSU *Division of Information Technology Security Policies* require users to set strong account passwords to protect computers from being accessed by unauthorized people. Computer accounts with blank passwords have no protection against someone with physical access to the computer. A strong password is one that has at least twelve characters and is made up of upper and lower case letters plus special characters (e.g., "@", "%", spaces, and punctuation marks) and/or numbers.

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

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

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

The ABS director stated that the password and login parameters set in the payroll and child care systems were set according to the options available. She added that in the child care system, there was a temporary account/password setup for temporary staff.

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

### **Recommendation 6**

We recommend that the campus:

- a. Set effective password and login security parameters for the ADP payroll and child care systems in accordance with campus and leading information security industry guidelines and perform an assessment of password security parameters for all other systems administered by ABS.
- b. Eliminate all generic user accounts and establish a unique user account for each user in the child care system.

### **Campus Response**

We concur. ABS:

- a. Is currently working with ADP to convert to one of their web-based products which includes the enhanced security features noted. In addition, ABS is in the process of reviewing and migrating to a new childcare system product which will address increased password security.

Expected completion date: August 2010

- b. Will eliminate all generic user accounts in the childcare system and assign appropriate user accounts as needed.

Expected completion date: May 2010

## **THE UNIVERSITY CORPORATION, SAN FRANCISCO STATE**

### **FACILITIES AGREEMENTS**

Certain lease and sublease agreements between The University Corporation, San Francisco State (Corporation) and other entities had not been amended to reflect the new name of the auxiliary and/or did not include appropriate indemnification provisions.

We found that:

- ▶ Seven lease and sublease agreements were still executed in the former name of the auxiliary, San Francisco State University Foundation, Inc., and had not been amended to reflect its new name.
- ▶ Seven sublease agreements lacked indemnification provisions to specifically indemnify the State of California, CSU Trustees, and the campus. This is a repeat finding from the prior Auxiliary Organizations audit.

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 properly executed agreements.

EO 849, *California State University Insurance Requirements*, dated February 5, 2003, states that auxiliary organizations shall require certain levels of insurance and 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, arising out of, or in any way connected with the operations of the auxiliary.

The ABS director stated that the agreements that were still executed in the former name of the auxiliary were being individually changed as they were renewed or amended for other changes. She added that the lack of appropriate indemnification provisions was due to oversight.

The absence of current and complete written agreements and/or appropriate indemnification provisions increases the risk of misunderstandings and miscommunication regarding rights and responsibilities, and subjects the auxiliary and CSU to potential liability.

### **Recommendation 7**

We recommend that the Corporation:

- a. Promptly amend the cited agreements still executed in the former name of the auxiliary to reflect the new name of the auxiliary.
- b. Ensure that all future agreements include appropriate indemnification provisions.

### **Campus Response**

We concur. The Corporation will review and update agreements with the Corporations' name and appropriate indemnification clause.

Expected completion date: June 2010

## **FISCAL COMPLIANCE**

The Corporation did not record board-designated reserves within the general ledger in accordance with its reserve policy. This is a repeat finding from the prior Auxiliary Organizations audit.

The Corporation *Reserve Policy* states that annually, the Corporation Board of Directors shall review the fiscal viability of the organization to include an evaluation of the need for reserves in the following areas: working capital, contingencies, plant fund, planned future operations, redistribution of indirect cost, and presidential/university requests.

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 8.1.1.2 A-2, *Basis for Financial Standards and Fiscal Viability – Financial Statements*, states that annually each auxiliary governing board shall review the fiscal viability of the auxiliary organization to include an evaluation of the need for reserves in the following areas: a) working capital, b) current operations, c) capital replacement, and d) planned future operations.

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 a designated fund balance be recognized within an organization's general ledger.

The ABS director stated that the Corporation did not segregate its designated reserves within the general ledger because they had always been tracked manually and disclosed as part of the budget process annually with the board.

Failure to record designated reserve amounts according to the reserve policy increases the risk of misunderstandings and miscommunication regarding available reserves.

**Recommendation 8**

We recommend that the Corporation segregate designated reserves within its general ledger in accordance with its reserve policy.

**Campus Response**

We concur. The Corporation has created designated reserves within its general ledger in accordance with its reserve policy.

**PROPERTY AND EQUIPMENT**

Administration of Corporation property and equipment did not provide for timely disposition because property and equipment dispositions were only communicated to the campus ABS unit for removal from the general ledger once annually instead of at the time of disposition.

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

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

The ABS director stated that property and equipment dispositions have been processed once per year as part of their year-end closing process. She further stated that the Corporation performed an annual inventory during which project directors would identify items which had been disposed of during the year.

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

**Recommendation 9**

We recommend that the Corporation communicate the disposition of property and equipment to ABS at the time of disposition to ensure timely recording to the general ledger.

### **Campus Response**

We concur. The Corporation has coordinated and communicated all dispositions of property and equipment to ABS at the time of disposition.

## **TRUSTS AND OTHER LIABILITIES**

Certain campus program revenues may be inappropriately deposited to, and held in custody by, the Corporation. This is a repeat finding from the prior Auxiliary Organizations audit.

The Corporation financial statements as of June 30, 2009, indicated that the Corporation administered and maintained 352 custodial trust accounts totaling \$1,132,036. We reviewed 50 of these accounts for which trust account agreements were available and found that state/campus operating revenue funds may be inappropriately held by the Corporation in nearly all of the accounts.

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

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

The ABS director stated that a review of custodial trust funds had been previously completed and the Corporation believed that it had moved all state/campus operating funds to appropriate campus trust accounts.

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

### **Recommendation 10**

We recommend that the Corporation:

- a. Complete a review of all custodial trust accounts reflected as "deposits held for others" on its financial statements and determine, within 60 days, which accounts contain state/campus operating funds.
- b. Certify that none of the following specific and similar monies reside in Corporation trust accounts:

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

### **Campus Response**

We do not concur with the finding and recommended corrective actions. Executive Order 1000 states that it “supersedes Executive Order 648, 753, and 919 in their entirety.” We are interpreting the document as written and believe we are in compliance with EO 1000 as it pertains to our trust projects. The chancellor’s office has appointed a task force to review the executive orders and is currently developing additional policy directives related to fiscal affairs of non-General Fund receipts. When the new guidance is issued, the campus will immediately incorporate it into our processes and controls as appropriate.

Following the 2006 Auxiliary Organizations audit (referred to in the finding), the Corporation (formerly SFSU Foundation) performed a review of its trust projects and transferred projects to the campus as appropriate. The Corporation also implemented a review at initial project setup to ensure appropriate classification of new projects. The corrective actions were reviewed and the finding was cleared by the Office of the University Auditor. The Corporation continues to review its trust projects at initial setup to ensure it administers campus programs per published authority.

We have reviewed the 50 campus projects selected in the audit. These included the ten largest projects, and 48 percent of all Corporation projects. Due to fiscal year-end, annual financial audits and a major Common Financial System (CFS) common code conversion project, we would not be able to continue our review of all program accounts (currently 724 accounts) until October 2010. However, with the help of the Office of the University Auditor, a review of the accounts will commence on September 7, 2010. Upon completion of that review, we will transfer programs/funds to the campus as appropriate.

## ENDOWMENT ADMINISTRATION

Certain Corporation endowment files lacked executed endowment agreements and/or account set-up forms, and some endowment agreements did not delineate administrative fees.

We reviewed ten endowment files and found that:

- ▶ In two instances, endowment files did not contain fully executed endowment agreements.
- ▶ In three instances, endowment files did not contain the proper account set-up forms.
- ▶ In two instances, endowment agreements did not address the Corporation's administrative fees.

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

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

The ABS director stated that university advancement maintained e-mail correspondence with the donor's intention as support for establishment of the endowments. She further stated that Corporation endowment files contained the same information, which was considered sufficient. She added that administrative fees were addressed through an internal process but not within the formal agreement, and the lack of proper account set-up forms was due to oversight.

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

### **Recommendation 11**

We recommend that the Corporation:

- a. Ensure the completion of endowment agreements for all future endowments.
- b. Ensure that each endowment file contains an account set-up form.
- c. Update its endowment agreement to specifically address the Corporation's administrative fees.

**Campus Response**

We concur. The Corporation will ensure that all future endowments will have an endowment agreement, setup form, and address administrative fees.

Expected completion date: May 2010

## **FRANCISCAN SHOPS**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS**

The arrangement between Franciscan Shops (Shops) and a third-party service provider that performed physical inventory counts was not supported by a service agreement that included appropriate insurance and indemnification provisions.

A purchase order instead of a service agreement was used for a third-party service provider that performed physical inventory counts, and the purchase order did not reference the CSU General Provisions. As a result, insurance and indemnification provisions were not addressed.

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 for services be supported by complete, written agreements that incorporate appropriate insurance and indemnification provisions.

EO 849, *California State University Insurance Requirements*, dated February 5, 2003, states that auxiliary organizations shall require certain levels of insurance and 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, arising out of, or in any way connected with the operations of the auxiliary.

The Shops general manager stated his belief that the purchase order served as the service agreement and that management was not aware of requirements to reference the CSU General Provisions.

The absence of a complete, written agreement that incorporates appropriate insurance and indemnification provisions increases the risk of misunderstandings and miscommunication regarding rights and responsibilities, and subjects the auxiliary and CSU to potential liability.

#### **Recommendation 12**

We recommend that Shops ensure that all future agreements with third parties for inventory services include appropriate insurance and indemnification provisions.

### **Campus Response**

We concur. Management has adopted a requirement for all service agreements wherein all contractors entering into service agreements are required to review, acknowledge, and agree to the terms and conditions as set forth in “SFSU Bookstore Provisions for Acquisitions of Goods,” “SFSU Bookstore Provisions for Information Technology Acquisitions,” or “SFSU Bookstore Provisions for Service Acquisitions” depending on the nature of the contract.

### **SEGREGATION OF DUTIES**

Certain duties and responsibilities related to the processing of human resources and payroll transactions were not adequately segregated at Shops.

We found that two Shops employees with access to one administrator account in the Ceridian payroll system had access to perform incompatible functions. Specifically, this access allowed the users to create new employees, terminate existing employees, process payroll transactions, process time and attendance, receive and review payroll warrant registers for irregularities, and reconcile payroll accounts to the general ledger.

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 8.9.6, *Payroll*, states that the auxiliary should establish a written control system that ensures payroll preparation is segregated from the general ledger function and other payroll functions such as hiring authorization, timekeeping, and distribution of checks.

The Shops general manager stated that management was not aware of this violation of responsible segregation of duties control.

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

### **Recommendation 13**

We recommend that Shops appropriately segregate certain human resources and payroll processing functions or institute mitigating procedures as approved by the campus CFO.

### **Campus Response**

We concur. Shops has signed a contract with a new payroll/HR processing firm for a new system with adequate controls.

Expected completion date: June 2010

## **PERSONNEL AND PAYROLL**

### **PAYROLL RECONCILIATION**

Payroll tax reconciliations were not timely reviewed by Shops management.

We reviewed the last four quarterly payroll tax reconciliations dated September 30, 2008, December 31, 2008, March 31, 2009, and June 30, 2009, and found that all four reconciliations were not reviewed and signed by management until August 3, 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 8.9.6, *Payroll*, states that the auxiliary should establish a written system that enables proper payroll deductions, collection and timely remittance of payroll taxes, and federal and state reporting.

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 timely review of payroll tax reconciliations by an independent manager.

The Shops controller stated that Shops' practice was to sign-off on all four quarterly returns after year end, rather than after each quarter.

Untimely review of payroll tax reconciliations increases the risk that errors and irregularities will not be detected in a timely manner.

### **Recommendation 14**

We recommend that Shops management review and approve payroll tax reconciliations in a timely manner, at least quarterly.

### **Campus Response**

We concur. Shops management will review and sign off on quarterly payroll tax returns and reconciliations within five business days of receipt.

## EMPLOYEE LEAVE

Employee leave accounting required improvement at Shops.

We found that:

- ▶ Employee vacation and sick leave accounting was recorded and tracked via one Excel spreadsheet maintained locally on one employee's computer, which was not electronically backed up on any periodic basis.
- ▶ Monthly updates to employee vacation and sick leave balances were not reviewed or reconciled by an independent manager subsequent to the payroll accountant's data entry.
- ▶ Adjustments to employee vacation and sick leave accrual rates were not approved by an independent manager.

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 8.9.10, *Computer Controls*, states that the auxiliary should establish written policies and practices that define processing controls, specifically, transaction edit checks, integrity of data files, reconciliation requirements, and error logs, as well as ensure backup mechanisms.

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

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 backing up any critical data residing on auxiliary systems and/or in files.

The Shops general manager stated that that management maintains hard-copy backup files of employee leave data and was unaware that an additional electronic backup was not occurring. He further stated that management had lost oversight ensuring independent manager review of updates and adjustments to leave records.

Failure to maintain adequate control over employee vacation and sick leave accounting increases the risk of lost data and errors and irregularities, which may under or over compensate employees and expose Shops to increased liability.

### **Recommendation 15**

We recommend that Shops:

- a. Implement stronger controls to maintain the integrity of employee vacation and sick leave accounting data, including routine electronic backup.
- b. Ensure that monthly updates and adjustments to employee vacation and sick leave balances and accrual rates are reviewed or reconciled, and approved by an independent manager subsequent to the data entry.

### **Campus Response**

We concur. Shops has signed a contract with a new payroll/HR processing firm for a new system with adequate controls. Implementation and training on the new system will take about four months.

Expected completion date: June 2010

## **INFORMATION TECHNOLOGY**

### **INFORMATION SECURITY TRAINING AND DATA CONFIDENTIALITY FORMS**

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

The SFSU *Confidentiality and Information Security Plan* states that all SFSU and auxiliary organization employees will receive employee/student confidentiality training as directed by the associate vice president for human resources, safety and risk management and the university registrar when feasible and deemed necessary. The appropriate custodian of records will provide training for employees approved for additional security access to employee, student, and/or financial confidential data. Training shall include controls and procedures to prevent employees from providing confidential information to an unauthorized individual or entity and how to properly handle, store, and dispose of documents that contain personal identifying information. Training shall also include information to protect against destruction, loss, or damage to confidential information from potential environmental hazards such as fire, water, acts of nature, or technological failures. Custodians of records shall document employees who have received training.

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

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

The Shops general manager stated that management was unaware of any requirement to conduct information security awareness training or sign data confidentiality forms for all personnel with access to critical systems or protected data.

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

#### **Recommendation 16**

We recommend that Shops:

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

#### **Campus Response**

We concur. Shops management will:

- a. Implement a 20-minute online information and system security awareness teaching module (offered by a contractor to all CSU auxiliary organizations) that is now required of all employees with access to confidential information or system screens beyond “read only” query level.
- b. Update its data confidentiality form required of all employees with access to critical systems and protected data to strengthen protection based on current standards.
- c. Obtain completed forms from personnel who currently have access to such data.

Expected completion date: April 2010

## **PASSWORD SECURITY**

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

We found that the password and login security parameters for the payroll system (including the human resources/payroll module and the time and attendance module) did not enforce any minimum password length, password complexity, periodic expiration, or login security.

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

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

The Shops general manager stated that management was unaware of the password and login security weaknesses in the payroll system.

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

### **Recommendation 17**

We recommend that Shops set effective password and login security parameters for the payroll system in accordance with security industry guidelines and perform an assessment of password security parameters for all other Shops systems.

### **Campus Response**

We concur. Shops has signed a contract with a new payroll/HR processing firm for a new system with an automated vacation and sick leave bookkeeping function including adequate controls.

Expected completion date: June 2010

## USER ACCESS

User access to Shops systems was not adequately reviewed or administered.

We found that:

- ▶ Shops did not perform periodic, documented management reviews of user access privileges within all Shops systems and applications containing protected data.
- ▶ Only one administrator account was used by two employees within the payroll system human resources/payroll module.
- ▶ There were many supervisor accounts with the capability to approve payroll within the payroll system time and attendance module. However the old/terminated supervisor accounts were neither removed nor was access to the accounts restricted.

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

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

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

The Shops general manager stated that the information systems manager conducts regular reviews of user access privileges, but management was unaware of any CSU requirement for periodic, documented reviews. He added that management was unaware two supervisors were sharing one password in the third-party payroll system and was unaware terminated supervisor accounts were not being deleted.

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

### **Recommendation 18**

We recommend that Shops:

- a. Conduct periodic, documented management reviews of user access for all systems containing protected data, at least annually.
- b. Assign unique user accounts to all employees requiring system access.
- c. Develop a formal process for disabling user accounts that no longer require access to systems.

### **Campus Response**

We concur. Shops management will:

- a. Conduct periodic, documented reviews of user access for all systems containing protected data.
- b. Enforce unique user accounts for all system users.
- c. Formalize its process for disabling user accounts that no longer require access to systems.

Expected completion date: May 2010

## **ENVIRONMENTAL CONTROLS**

The Shops server room lacked fire or smoke detection devices and was equipped with a problematic fire suppression system for a room storing critical servers/systems.

We found that:

- ▶ The server room was not equipped with fire or smoke detectors.
- ▶ The server room was equipped with a water-sprinkler system, which could be detrimental to the electrical equipment housed in the server room.

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

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that appropriate fire detection and suppression equipment be maintained within the premises of server rooms at all times.

The Shops general manager stated that the lack of fire and smoke detectors was due to oversight, but added that he had been informed during 1999-2000 construction that waterless fire detection and suppression systems were not up to building codes. He further stated that during the audit, management learned from the state fire marshal that such systems are now available and Shops began seeking bids for conversion to a waterless fire detection and suppression system.

Failure to maintain appropriate fire detection and suppression devices in the server room increases the risk of unsuccessful detection and suppression of a fire and/or damage to critical systems, which may expose employees to dangerous conditions and result in the loss of critical systems.

### **Recommendation 19**

We recommend that Shops:

- a. Install a fire and/or smoke detection system in the server room.
- b. Evaluate the feasibility of another means of fire suppression or consider relocation of Shops servers to the campus data center.

### **Campus Response**

We concur. Shops management is in the process of engaging a campus-approved contractor to install an integrated early warning smoke detection system and time delay water-based fire suppression system integrated with automatic electronic notification to campus police. In addition, it has evaluated the cost-effectiveness and practicality of hosting the Shops servers remotely in a facility protected by adequate environmental and fire controls; and has determined option/recommendation (a) serves the needs of Shops best.

Expected completion date: May 2010

## **SYSTEM BACKUPS**

The Shops process to backup payroll data transmitted to an off-site service provider was neither effective nor adequately secure.

We reviewed the daily backup process for payroll data and found that:

- ▶ All payroll data was transmitted to an off-site service provider where it was contractually required to be backed up by the service provider. As a result, local backup of this payroll data was redundant.
- ▶ The local backup file created by the payroll manager could not be opened for audit review.

- ▶ The local backup file was stored on an external zip drive and was not required to be encrypted even though it contained protected employee data. In addition, the local backup file was kept next to the workstation instead of being secured in a locked cabinet or safe.

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 operable backup files, secure local and off-site storage of backups, and encryption of protected data contained on auxiliary backups.

The Shops general manager stated that management was not fully aware of the local backup process, and also had never tested the backup system. He further stated that management had lost oversight of the controls for the local backups and had no knowledge of whether or not the backup drive was encrypted. He added that management was unaware of the need for secure storage of these backups.

Inadequate availability, security, and storage of system backups increases the risk that auxiliary systems will not be recovered in the event of a disaster, or that protected data will be compromised.

### **Recommendation 20**

We recommend that Shops reevaluate the process of local backups for payroll data transmitted to the off-site service provider, and consider the necessity of maintaining local backups. If deemed necessary, ensure that the local backups are operable and appropriately encrypted and secured.

### **Campus Response**

We concur. Shops has signed a contract with a new payroll/HR processing firm for a new system with a remotely hosted server and robust data backup capabilities.

Expected completion date: June 2010

## E-MAIL SYSTEMS

Shops e-mail policies and procedures were not documented, and password security controls were not adequate.

We noted that:

- ▶ Shops had not developed an administrative e-mail policy, standards, or guidelines to address the security, management, ownership, backup, and record retention of e-mail hosted remotely by a third party.
- ▶ Shops had not developed an end-user acceptable e-mail usage policy that outlines user responsibilities and restricts employees from certain activities such as sending protected data via e-mail.
- ▶ Password security parameters for the third party e-mail system only enforced a minimum password length of six characters and did not enforce any password complexity, periodic expiration, or login security controls.

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 sufficient documentation of administrative and end-user policies and procedures and adequate password and login security controls for e-mail systems.

The Shops general manager stated that the management information systems manager had agreed to terms and conditions of the third party, but never developed policies, standards, or guidelines addressing security, management, ownership, backup, and record retention. He added that management had not recognized the need to develop a formal policy on e-mail usage or storage. He further stated that management was unaware of the limits of password security management with the third party hosting Shops' e-mail solution.

The lack of documented administrative and end-user policies and procedures increases the risk of unauthorized and/or inappropriate use of e-mail systems, while insufficient password and login parameters may compromise the authentication credentials of user accounts, which increases the risk of unauthorized access to auxiliary information and confidential data.

**Recommendation 21**

We recommend that Shops:

- a. Develop administrative e-mail policies, standards, or guidelines to address the security, management, ownership, backup, and record retention of e-mail hosted remotely by a third party.
- b. Develop an end-user acceptable e-mail usage policy that outlines user responsibilities and restrictions.
- c. Set effective password and login security parameters for the third-party e-mail system in accordance with campus and security industry guidelines.

**Campus Response**

We concur. Shops management will:

- a. Develop administrative e-mail policies, standards, or guidelines to address the security, management, ownership, backup, and record retention of the Shops' email system.
- b. Review and revise the Shops' email usage policy to outline user responsibilities and restrictions.
- c. Review and strengthen password and login security parameters for the Shops' email system to reflect campus and security industry guidelines.

Expected completion date: May 2010

## **ASSOCIATED STUDENTS OF SAN FRANCISCO STATE UNIVERSITY**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS**

Certain agreements between Associated Students of San Francisco State University (AS) and independent contractors did not include appropriate insurance and indemnification provisions.

We reviewed five independent contractor agreements and found that all five did not contain proper insurance provisions and lacked indemnification provisions to specifically indemnify the CSU Trustees, the campus, and the State of California.

EO 849, *California State University Insurance Requirements*, dated February 5, 2003, states that auxiliary organizations shall require certain levels of insurance and 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, arising out of, or in any way connected with the operations of the auxiliary.

The AS executive director stated that failure to include the proper insurance and indemnification provisions in the independent contractor agreements was due to oversight.

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

#### **Recommendation 22**

We recommend that AS ensure that all future agreements include appropriate insurance and indemnification provisions.

#### **Campus Response**

We concur. AS will ensure that all future agreements include appropriate insurance and indemnification provisions.

Expected completion date: May 2010

## **OPERATIONAL COMPLIANCE**

### **POLICIES AND PROCEDURES**

AS had not developed written policies and procedures to address the accounting and processing of accounts receivable.

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

- ▶ Creation of invoices.
- ▶ Aging and collection of past-due accounts receivable.
- ▶ Valuation of allowance for doubtful accounts receivable.
- ▶ Write-off of uncollectible 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 accounting and processing of accounts receivable.

The AS executive director stated that the lack of a formalized policy and procedure related to accounts receivable was due to oversight.

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

#### **Recommendation 23**

We recommend that the AS develop written policies and procedures to address the accounting and processing of accounts receivable.

#### **Campus Response**

We concur. AS will develop written policies and procedures to address accounting and processing of accounts receivable.

Expected completion date: May 2010

## **RISK MANAGEMENT**

AS had not developed a written risk management policy.

We found that AS did not have a written risk management policy that addressed an ongoing process to proactively identify risks, analyze the frequency and severity of identified risks, and to implement a risk mitigation program which 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 AS executive director stated that the failure to have a written risk management policy was due to oversight.

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

### **Recommendation 24**

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

### **Campus Response**

We concur. AS will develop and adopt a risk management policy.

Expected completion date: July 2010

## **PERSONNEL AND PAYROLL**

AS did not perform a detailed, documented reconciliation of AS-generated payroll reports against the ADP payroll records processed by ABS.

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 8.9.6, *Payroll*, states that the auxiliary should establish a written system that ensures proper authorization, approval, and documentation of new hires, changes in employment, salary and wage rates, and payroll deductions.

The AS associate executive director was unaware that AS-generated payroll reports needed to be reconciled against ADP payroll records after ABS processed the payroll.

Insufficient reconciliation between AS-generated payroll reports and the ADP payroll records processed by ABS limits auxiliaries the ability to detect errors and irregularities, increases the likelihood of loss of funds, and compromises accountability.

### **Recommendation 25**

We recommend that AS perform detailed, documented reconciliations of AS-generated payroll reports against the ADP payroll records processed by ABS.

### **Campus Response**

We concur. AS will review AS-generated payroll reports against the ADP payroll records processed by ABS.

Expected completion date: June 2010

## **PROPERTY AND EQUIPMENT**

Administration of AS property and equipment did not provide for timely disposition because property and equipment dispositions were only communicated to the campus ABS unit for removal from the general ledger once annually instead of at the time of disposition.

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

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

The AS business office manager stated that he was unaware that reporting property and equipment dispositions once annually was insufficient.

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

**Recommendation 26**

We recommend that AS communicate the disposition of property and equipment to ABS at the time of disposition to ensure timely recording to the general ledger.

**Campus Response**

We concur. AS will coordinate the disposition of property and equipment with ABS accordingly.

Expected completion date: May 2010

## **SAN FRANCISCO STATE UNIVERSITY STUDENT CENTER**

### **OPERATIONAL COMPLIANCE**

The San Francisco State University Student Center (Student Center) had not developed written policies and procedures to fully address the accounting and processing of accounts receivable.

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

- ▶ Creation of invoices.
- ▶ Aging and collection of past-due accounts receivable.
- ▶ Valuation of allowance for doubtful accounts receivable.
- ▶ Write-off of uncollectible 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 accounting and processing of accounts receivable.

The Student Center associate director of business/finance stated that the room reservations policy as well as the vendor sublease agreements outlined collection efforts procedures. She further stated that write-offs of outstanding accounts receivable begin as a process from ABS near each fiscal year end when the managing director signs off on the balances designated for write off; however, this process was not documented.

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

#### **Recommendation 27**

We recommend that the Student Center develop written policies and procedures to address the accounting and processing of accounts receivable.

#### **Campus Response**

We concur. The Student Center will revise its accounting policies to include the accounting and processing of the four mentioned aspects of accounts receivable and will present those for approval to the Student Center Governing Board at its June 2010 meeting.

Expected completion date: June 2010

## **PETTY CASH AND CHANGE FUNDS**

Administration of Student Center change and petty cash funds required improvement.

We reviewed the \$7,000 safe/change fund and the \$500 petty cash fund and found that:

- ▶ There were total change fund shortages of \$537 and \$616 in fiscal years 2007/08 and 2008/09, respectively, without definitive explanation for the cause of the shortages.
- ▶ Independent cash counts of these change and petty cash funds were only performed on an annual basis.
- ▶ Change funds for the information desk (five bags with \$250 each) and the games room (five bags with \$150 each) were not physically counted during these annual independent cash counts.

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 change and petty cash funds, including periodic, independent cash counts and documentation of management investigation of shortages.

The Student Center accounting supervisor stated that management has not come up with a definitive explanation for why the shortage has occurred. She added that management requested additional counts from the independent verifier during the year. She further stated that during the count, the independent verifier was aware that the smaller bags are counted internally in double custody daily, and opted not to open the bags and re-count the funds.

Inadequate administration of change and petty cash funds increases the risk of loss or misappropriation of funds.

### **Recommendation 28**

We recommend that the Student Center:

- a. Develop and implement a written procedure to ensure documented management review and investigation of shortages.
- b. Perform independent cash counts of all change and petty cash funds on a more frequent basis, at least quarterly.

### **Campus Response**

We concur. The Student Center will:

- a. Develop a written policy to formalize the procedure(s) regarding investigation of shortages.
- b. Expand the current accounting policy to address the frequency of review of the cash counts of change and petty cash funds and to ensure all funds are physically counted during each review.

Both policies will be presented to the Student Center Governing Board for approval at its June 2010 meeting.

Expected completion date: June 2010

## **PERSONNEL AND PAYROLL**

### **POLICIES AND PROCEDURES**

The Student Center did not have written policies or procedures pertaining to the semimonthly payroll process.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.6, *Payroll*, states that the auxiliary should establish a written system that ensures proper authorization, approval, and documentation of new hires, changes in employment, salary and wage rates, and payroll deductions.

The Student Center associate director of business/finance stated that the HR/payroll manager had written notes on the payroll process, but because HR was a department of one, formalization of the notes was not completed.

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

### **Recommendation 29**

We recommend that the Student Center develop written policies and procedures pertaining to the payroll process.

### **Campus Response**

We concur. The Student Center will expand its current HR policy manual to include the steps required for processing of the semimonthly payroll and will present it to the Student Center Governing Board for approval at its June 2010 meeting.

Expected completion date: June 2010

## **PAYROLL RECONCILIATION**

The Student Center did not perform a detailed, documented reconciliation of Student Center-generated payroll reports against the ADP payroll records processed by ABS.

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 8.9.6, *Payroll*, states that the auxiliary should establish a written system that ensures proper authorization, approval, and documentation of new hires, changes in employment, salary and wage rates, and payroll deductions.

The Student Center associate director of business/finance stated that other procedures were in place for the collection and distribution of payroll checks that provide for a system of checks and balances between the Student Center accounting department and ABS.

Insufficient reconciliation between Student Center-generated payroll reports and ADP payroll records processed by ABS limits the auxiliary's ability to detect errors and irregularities, increases the likelihood of loss of funds, and compromises accountability.

### **Recommendation 30**

We recommend that the Student Center perform detailed, documented reconciliations of Student Center-generated payroll reports against the ADP payroll records processed by ABS.

### **Campus Response**

We concur. The Student Center will include in the development of the semimonthly payroll policy a component relating to document reconciliation of the Student Center generated payroll reports against ADP payroll records processed by ABS. This policy will be presented to the Student Center Governing Board for approval at its June 2010 meeting.

Expected completion date: June 2010

---

## **APPENDIX A: PERSONNEL CONTACTED**

### **Name**

### **Title**

#### **CAMPUS**

Robert A. Corrigan	President
Donna Blakemore	Associate Vice President, University Advancement
Lee Blitch	Vice President, University Advancement
Eva Du	Accountant, Auxiliary Business Services
Mig Hoffman	Information Security Officer
Lin Joe	Accountant, Auxiliary Business Services
Irina Krasnitskaya	Senior Gift Processor, Advancement Services
Michael Lam	Lead IT Consultant, Fiscal Affairs Business Systems
Jeanne Lee	Stewardship and Donor Relations Coordinator, Advancement Services
Leroy M. Morishita	Vice President and Chief Financial Officer, Administration and Finance
Mark Osborne	Interim Internal Auditor (At time of review)
Tammie Ridgell	Director, Auxiliary Business Services
Cora Wong	Director, Fiscal Affairs Business Systems

#### **SAN FRANCISCO STATE UNIVERSITY FOUNDATION**

Debra Chaw	Chief of Operations, University Advancement
------------	---------------------------------------------

#### **THE UNIVERSITY CORPORATION, SAN FRANCISCO STATE**

Vincent Cheung	Accounting Supervisor
Keith Churchill	Accounting Technician
Naum Korenfeld	Accounts Payable Technician
Tammie Ridgell	Director, Auxiliary Business Services
Anthony Victoria	Administrative Services Director
Agnes Wong Nickerson	Associate Vice President for Fiscal Affairs

#### **FRANCISCAN SHOPS**

Nazanin Calhoun	Customer Service/Administration Manager
Jim Chen	Computer Department Manager
Fred Eskridge	Information Systems Manager
Chris Farmer	Controller
Romeo Galang	Accounting Manager
Wendy Johnson	Textbook Manager
Lolita Ramos	Cash Control Supervisor
Robert Strong	General Manager
Nils Tagtstrom	Accounts Payable Technician
Ken White	General Books Manager
Amber Wilson	General Merchandise Manager
Brian Zimmerman	Associate General Manager

**ASSOCIATED STUDENTS OF SAN FRANCISCO STATE UNIVERSITY**

Jamila Ali	Associate Executive Director
Jason Bell	Director, Project Rebound
Veronica Castillo	Office Manager, Early Childhood Education Center
Mario Flores	Director, Project Connect
Sarah Johnson	Director, Early Childhood Education Center
Muata Kenyatta	Director, Performing Arts and Lectures
Peter Koo	Executive Director
Horace Montgomery	Leadership Development Coordinator
Alejandro Rios	Business Office Manager

**SAN FRANCISCO STATE UNIVERSITY STUDENT CENTER**

Edina Bajraktarevic	Associate Director of Business/Finance
Zoila Baltodano	Business Office Manager
Eleanor Callado	Accounting Supervisor
Guy Dalpe	Managing Director
Jeannette Peralta	Human Resources/Payroll Manager

## **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.



OFFICE OF THE PRESIDENT

1600 Holloway Avenue  
San Francisco, CA 94132

Phone: 415/338-1381

Fax: 415/338-6210

web: www.sfsu.edu

**REVISED RESPONSE**

July 12, 2010

RECEIVED  
UNIVERSITY AUDITOR

JUL 15 2010

THE CALIFORNIA STATE  
UNIVERSITY

Mr. Larry Mandel  
University Auditor  
The California State University  
401 Golden Shore  
Long Beach, California 90802-4275

Dear Mr. Mandel:

We have reviewed the Office of the University Auditor Report #09-17 on Auxiliary Organizations at San Francisco State University. Our responses to the recommendations are attached which will also be forwarded to your staff electronically. We are taking actions to implement the recommendations.

Documentation demonstrating implementation of recommendations already completed will be forwarded to you separately. Questions regarding the responses may be directed to Leroy M. Morishita, Executive Vice President and CFO for Administration & Finance, at 415/338-2521 or Heather Boshears, Internal Auditor, at 415/405-4343.

Sincerely,

A handwritten signature in black ink, appearing to read "Robert A. Corrigan".

Robert A. Corrigan  
President

HB/id  
Attachments

cc: Leroy M. Morishita, Executive Vice President and CFO, Administration and Finance  
J. E. (Penny) Saffold, Vice President, Dean of Students/Student Affairs  
Jonathan Rood, Associate Vice President and CIO, Division of Information Technology  
Agnes Wong Nickerson, Interim Associate Vice President, Fiscal Affairs  
Guy Dalpe, Managing Director, Cesar Chavez Student Center  
Peter Koo, Executive Director, Associated Students, Inc.  
Robert Strong, General Manager, Franciscan Shops  
Tammie Ridgell, Director, Auxiliary Business Services  
Mig Hofmann, Information Security Officer, DoIT (recommendations 4 & 5)  
Christopher Bomar, Executive Assistant, Administration and Finance  
Heather Boshears, Internal Auditor

**AUXILIARY ORGANIZATIONS**  
**SAN FRANCISCO STATE UNIVERSITY**

**Audit Report 09-17**

**CAMPUS**

**OPERATING AND ADMINISTRATIVE AGREEMENTS**

**Recommendation 1**

We recommend that the campus establish a written agreement with the payroll service provider; and for all vendor service agreements relating to access to protected records or data, consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities and the confidentiality of data.

**Campus Response**

We concur. Auxiliary Business Services (ABS) will work with the payroll service provider and incorporate the CSU General Provisions for Information Technology Acquisitions via the purchase order provided to the vendor. Expected completion date: July 2010.

**SEGREGATION OF DUTIES**

**Recommendation 2**

We recommend that the campus appropriately segregate certain payroll and personnel processing functions or institute mitigating procedures approved by the campus chief financial officer (CFO).

**Campus Response**

We concur. Auxiliary Business Services has taken the appropriate steps to ensure mitigating controls exist outside of the system:

- All input information is initiated by the Human Resource function of each auxiliary.
- All new employees created or employees records changed are only initiated with the appropriate documentation. We have implemented a new step to assist in preventing erroneous checks from being created. Before payroll is processed a change report is produced from the payroll system and reviewed with the supported documentation by the Director of ABS or designee.

The approval of the mitigating procedures outlined above will be obtained from the campus CFO. Expected completion date: June 2010.

## PROPERTY AND EQUIPMENT

### Recommendation 3

We recommend that the campus record AS and Student Center property and equipment additions when received and record the related depreciation expense on a more frequent basis, at least quarterly.

### Campus Response

We concur. Auxiliary Business Services have implemented recording additions on a quarterly basis as well as recording the related depreciation expense.

## INFORMATION TECHNOLOGY

### PROTECTED DATA ASSESSMENT

#### Recommendation 4

We recommend that the campus ensure that the auxiliaries perform an initial, and then annual, assessment and inventory of protected data on all systems to determine the existence of any protected data and the need for appropriate logical and physical security measures.

### Campus Response

We concur. The campus biennial survey of all campus systems will include auxiliaries. Expected completion date: July 2010.

### PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

#### Recommendation 5

We recommend that the campus and auxiliaries:

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

**Campus Response**

We concur. The campus will request its Auxiliary Organizations to review their contractual requirements, if appropriate, with their legal counsel; and review segmentation of any electronic transmission which may present liability to the campus. Expected completion date: July 2010.

**PASSWORD SECURITY AND USER ACCESS****Recommendation 6**

We recommend that the campus:

- a. Set effective password and login security parameters for the ADP payroll and child care systems in accordance with campus and leading information security industry guidelines and perform an assessment of password security parameters for all other systems administered by ABS.
- b. Eliminate all generic user accounts and establish a unique user account for each user in the child care system.

**Campus Response**

We concur. Auxiliary Business Services (ABS):

- a. Is currently working with ADP to convert to one of their web based products which includes the enhanced security features noted. In addition, ABS is in the process of reviewing and migrating to a new childcare system product which will address increased password security. Expected completion date: August 2010.
- b. Will eliminate all generic user accounts in the child care system and assign appropriate user accounts as needed. Expected completion date: May 2010.

**THE UNIVERSITY CORPORATION, SAN FRANCISCO STATE**

**FACILITIES AGREEMENTS**

**Recommendation 7**

We recommend that the Corporation:

- a. Promptly amend the cited agreements still executed in the former name of the auxiliary to reflect the new name of the auxiliary.
- b. Ensure that all future agreements include appropriate indemnification provisions.

**Campus Response**

We concur. The Corporation will review and update agreements with the Corporations' name and appropriate indemnification clause. Expected completion date: June 2010.

**FISCAL COMPLIANCE**

**Recommendation 8**

We recommend that the Corporation segregate designated reserves within its general ledger in accordance with its reserve policy.

**Campus Response**

We concur. The Corporation has created designated reserves within its general ledger in accordance with its reserve policy.

**PROPERTY AND EQUIPMENT**

**Recommendation 9**

We recommend that the Corporation communicate the disposition of property and equipment to ABS at the time of disposition to ensure timely recording to the general ledger.

**Campus Response**

We concur. The Corporation has coordinated and communicated all dispositions of property and equipment to ABS at the time of disposition.

## TRUSTS AND OTHER LIABILITIES

### Recommendation 10

We recommend that the Corporation:

- a. Complete a review of all custodial trust accounts reflected as “deposits held for others” on its financial statements and determine, within 60 days, which accounts contain state/campus operating funds.
- b. Certify that none of the following specific and similar monies reside in Corporation trust accounts:
  - Contracts and grants awarded to the university.
  - ~~Pre-award indirect cost recovery reimbursements.~~
  - Corporation net operating surplus designated for use by the campus.
  - Fees for continuing education courses provided by the university.
  - Fees for university events, workshops, conferences, institutes, special projects, and programs.
  - Reimbursements for services and products provided to auxiliary enterprises and organizations paid from General Fund and/or CSU operating fund monies.
  - Rental fees for university facilities, except those facilities that have been leased to the auxiliary by the campus.
  - Student fees and other general fees pursuant to the CSU student fee policy.
  - Monies held by the Corporation via contract with the campus.
- c. Submit to the Office of the University Auditor, within 60 days, a list of those trust accounts which have been deemed appropriate to remain in the custody of the Corporation and comprehensive documentation to support the sources of funds for those trust accounts.
- d. Move those state/operating funds identified in “a” above to campus accounts within six months.

### Campus Response

We do not concur with the finding and recommended corrective actions. Executive Order 1000 states that it “supersedes Executive Order 648, 753, and 919 in their entirety”. We are interpreting the document as written and believe we are in compliance with E.O. 1000 as it pertains to our trust projects. The Chancellor’s Office has appointed a task force to review the executive orders and is currently developing additional policy directives related to fiscal affairs of non-general fund receipts. When the new guidance is issued the campus will immediately incorporate it into our processes and controls as appropriate.

Following the 2006 Auxiliary Organizations audit (referred to in the finding) the Corporation (formerly SFSU Foundation) performed a review of its trust projects and transferred projects to the campus as appropriate. The Corporation also implemented a review at initial project setup to ensure appropriate classification of new projects. The corrective actions were reviewed and the finding was cleared by the Office of the University Auditor. The Corporation continues to review its trust projects at initial set up to ensure it administers campus programs per published authority.

We have reviewed the 50 campus projects selected in the audit. These included the ten largest projects, and 48% of all Corporation projects. Due to fiscal year-end, annual financial audits and a major CFS common code conversion project, we would not be able to continue our review of all program accounts (currently 724 accounts) until October 2010. However, with the help of the Office of the University Auditor, a review of the accounts will commence on September 7, 2010. Upon completion of that review, we will transfer programs/funds to the campus as appropriate.

## **ENDOWMENT ADMINISTRATION**

### **Recommendation 11**

We recommend that the Corporation:

- a. Ensure the completion of endowment agreements for all future endowments.
- b. Ensure that each endowment file contains an account set-up form.
- c. Update its endowment agreement to specifically address the Corporation's administrative fees.

### **Campus Response**

We concur. The Corporation will ensure that all future endowments will have an endowment agreement, set-up form, and address administrative fees. Expected completion date: May 2010.

## FRANCISCAN SHOPS

### OPERATING AND ADMINISTRATIVE AGREEMENTS

#### **Recommendation 12**

We recommend that Shops ensure that all future agreements with third parties for inventory services include appropriate insurance and indemnification provisions.

#### **Campus Response**

We concur. Management has adopted a requirement for all service agreements wherein all contractor entering into service agreements are required to review, acknowledge and agree to the terms and conditions as set forth in “SFSU Bookstore Provisions for Acquisitions of Goods,” “SFSU Bookstore Provisions for Information Technology Acquisitions,” or “SFSU Bookstore Provisions for Service Acquisitions” depending on the nature of the contract.

### SEGREGATION OF DUTIES

#### **Recommendation 13**

We recommend that Shops appropriately segregate certain human resources and payroll processing functions or institute mitigating procedures as approved by the campus CFO.

#### **Campus Response**

We concur. The Shops has signed a contract with a new payroll / HR processing firm for a new system with adequate controls. Expected completion date: June 2010.

### PERSONNEL AND PAYROLL

#### **PAYROLL RECONCILIATION**

#### **Recommendation 14**

We recommend that Shops management review and approve payroll tax reconciliations in a timely manner, at least quarterly.

#### **Campus Response**

We concur. Shops management will review and sign off on quarterly payroll tax returns & reconciliations within 5 business days of receipt.

## **EMPLOYEE LEAVE**

### **Recommendation 15**

We recommend that Shops:

- a. Implement stronger controls to maintain the integrity of employee vacation and sick leave accounting data, including routine electronic backup.
- b. Ensure that monthly updates and adjustments to employee vacation and sick leave balances and accrual rates are reviewed or reconciled, and approved by an independent manager subsequent to the data entry.

### **Campus Response**

We concur. The Shops has signed a contract with a new payroll / HR processing firm for a new system with adequate controls. Implementation and training on the new system will take about 4 months. Expected completion date: June 2010.

## **INFORMATION TECHNOLOGY**

### **INFORMATION SECURITY TRAINING AND DATA CONFIDENTIALITY FORMS**

#### **Recommendation 16**

We recommend that Shops:

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

#### **Campus Response**

We concur. Shops management will:

- a. Implement a 20 minute online information & system security awareness teaching module (offered by a contractor to all CSU auxiliary organizations) that is now required of all employees with access to confidential information or system screens beyond “read only” query level.
- b. Update its data confidentiality form required of all employees with access to critical systems and protected data to strengthen protection based on current standards.
- c. Obtain completed forms from personnel who currently have access to such data.

Expected completion date: April 2010.

## **PASSWORD SECURITY**

### **Recommendation 17**

We recommend that Shops set effective password and login security parameters for the payroll system in accordance with security industry guidelines and perform an assessment of password security parameters for all other Shops systems.

### **Campus Response**

We concur. The Shops has signed a contract with a new payroll / HR processing firm for a new system with an automated vacation and sick leave bookkeeping function including adequate controls. Expected completion date: June 2010.

## **USER ACCESS**

### **Recommendation 18**

We recommend that Shops:

- a. Conduct periodic, documented management reviews of user access for all systems containing protected data, at least annually.
- b. Assign unique user accounts to all employees requiring system access.
- c. Develop a formal process for disabling user accounts that no longer require access to systems.

### **Campus Response**

We concur. Shops management will:

- a. Conduct periodic, documented reviews of user access for all systems containing protected data.
- b. Enforce unique user accounts for all system users.
- c. Formalize its process for disabling user accounts that no longer require access to systems.

Expected completion date: May 2010.

## ENVIRONMENTAL CONTROLS

### Recommendation 19

We recommend that Shops:

- a. Install a fire and/or smoke detection system in the server room.
- b. Evaluate the feasibility of another means of fire suppression or consider relocation of Shops servers to the campus data center.

### Campus Response

We concur. Shops management is in the process of engaging a campus approved contractor to install an integrated early warning smoke detection system and time delay water-based fire suppression system integrated with automatic electronic notification to campus police. In addition, it has evaluated the cost-effectiveness and practicality of hosting the Shops servers remotely in a facility protected by adequate environmental and fire controls; and has determined option/recommendation (a) serves the needs of the Shops best. Expected completion date: May 2010.

## SYSTEM BACKUPS

### Recommendation 20

We recommend that Shops reevaluate the process of local backups for payroll data transmitted to the off-site service provider, and consider the necessity of maintaining local backups. If deemed necessary, ensure that the local backups are operable and appropriately encrypted and secured.

### Campus Response

We concur. The Shops has signed a contract with a new payroll / HR processing firm for a new system with a remotely hosted server and robust data backup capabilities. Expected completion date: June 2010.

## E-MAIL SYSTEMS

### Recommendation 21

We recommend that Shops:

- a. Develop administrative e-mail policies, standards, or guidelines to address the security, management, ownership, backup, and record retention of e-mail hosted remotely by a third party.
- b. Develop an end-user acceptable e-mail usage policy that outlines user responsibilities and restrictions.
- c. Set effective password and login security parameters for the third-party e-mail system in accordance with campus and security industry guidelines.

### **Campus Response**

We concur. Shops management will:

- a. Develop administrative e-mail policies, standards, or guidelines to address the security, management, ownership, backup, and record retention of the Shops' email system.
- b. Review and revise the Shops' email usage policy to outline user responsibilities and restrictions.
- c. Review and strengthen password and login security parameters for the Shops' email system to reflect campus and security industry guidelines.

Expected completion date: May 2010.

**ASSOCIATED STUDENTS OF SAN FRANCISCO STATE UNIVERSITY****OPERATING AND ADMINISTRATIVE AGREEMENTS****Recommendation 22**

We recommend that AS ensure that all future agreements include appropriate insurance and indemnification provisions.

**Campus Response**

We concur. The Associated Students will ensure that all future agreements include appropriate insurance and indemnification provisions. Expected completion date: May 2010.

**OPERATIONAL COMPLIANCE****POLICIES AND PROCEDURES****Recommendation 23**

We recommend that the AS develop written policies and procedures to address the accounting and processing of accounts receivable.

**Campus Response**

We concur. The Associated Students will develop written policies and procedures to address accounting and processing of accounts receivable. Expected completion date: May 2010.

**RISK MANAGEMENT****Recommendation 24**

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

**Campus Response**

We concur. The Associated Students will develop and adopt a risk management policy. Expected completion date: July 2010.

## PERSONNEL AND PAYROLL

### **Recommendation 25**

We recommend that AS perform detailed, documented reconciliations of AS-generated payroll reports against the ADP payroll records processed by ABS.

### **Campus Response**

We concur. The Associated Students will review AS-generated payroll reports against the ADP payroll records processed by ABS. Expected completion date: June 2010.

## PROPERTY AND EQUIPMENT

### **Recommendation 26**

We recommend that AS communicate the disposition of property and equipment to ABS at the time of disposition to ensure timely recording to the general ledger.

### **Campus Response**

We concur. The Associated Students will coordinate the disposition of property and equipment with ABS accordingly. Expected completion date: May 2010.

**SAN FRANCISCO STATE UNIVERSITY STUDENT CENTER****OPERATIONAL COMPLIANCE****Recommendation 27**

We recommend that the Student Center develop written policies and procedures to address the accounting and processing of accounts receivable.

**Campus Response**

We concur. The Student Center will revise its accounting policies to include the accounting and processing of the four mentioned aspects of Accounts Receivable and will present those for approval to the Student Center Governing Board at its June 2010 Board meeting. Expected completion date: June 2010.

**PETTY CASH AND CHANGE FUNDS****Recommendation 28**

We recommend that the Student Center:

- a. Develop and implement a written procedure to ensure documented management review and investigation of shortages.
- b. Perform independent cash counts of all change and petty cash funds on a more frequent basis, at least quarterly.

**Campus Response**

We concur. The Student Center will:

- a. Develop a written policy to formalize the procedure/s regarding investigation of shortages.
- b. Expand the current accounting policy to address the frequency of review of the cash counts of change and petty cash funds and to ensure all funds are physically counted during each review.

Both policies will be presented to the Student Center Governing Board for approval at its June 2010 meeting. Expected completion date: June 2010.

## **PERSONNEL AND PAYROLL**

### **POLICIES AND PROCEDURES**

#### **Recommendation 29**

We recommend that the Student Center develop written policies and procedures pertaining to the payroll process.

#### **Campus Response**

We concur. The Student Center will expand its current HR policy manual to include the steps required for processing of the semi-monthly payroll and will present it to the Student Center Governing Board for approval at its June 2010 meeting. Expected completion date: June 2010.

### **PAYROLL RECONCILIATION**

#### **Recommendation 30**

We recommend that the Student Center perform detailed, documented reconciliations of Student Center-generated payroll reports against the ADP payroll records processed by ABS.

#### **Campus Response**

We concur. The Student Center will include, in the development of the semi monthly payroll policy a component relating to document reconciliation of the Student Center generated payroll reports against ADP payroll records processed by ABS. This policy will be presented to the Student Center Governing Board for approval at its June 2010 meeting. Expected completion date: June 2010.

THE CALIFORNIA STATE UNIVERSITY  
OFFICE OF THE CHANCELLOR

BAKERSFIELD

CHANNEL ISLANDS

August 12, 2010

CHICO

DOMINGUEZ HILLS

**MEMORANDUM**

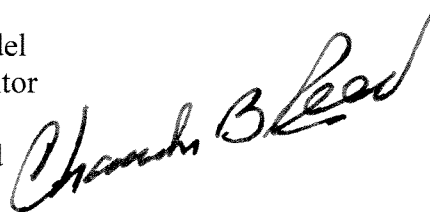
EAST BAY

TO: Mr. Larry Mandel  
University Auditor

FRESNO

FULLERTON

FROM: Charles B. Reed  
Chancellor



HUMBOLDT

SUBJECT: Draft Final Report 09-17 on *Auxiliary Organizations*,  
San Francisco State University

LONG BEACH

LOS ANGELES

MARITIME ACADEMY

In response to your memorandum of August 12, 2010, I accept the response as submitted with the draft final report on *Auxiliary Organizations*, San Francisco State University.

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/amd

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS