

**AUXILIARY ORGANIZATIONS**

**SAN JOSÉ STATE UNIVERSITY**

**Audit Report 10-02  
October 1, 2010**

---

**Members, Committee on Audit**

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

---

**Staff**

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

---

**BOARD OF TRUSTEES**

**THE CALIFORNIA STATE UNIVERSITY**

---

## CONTENTS

Executive Summary .....	1
Introduction.....	8
Background .....	8
Purpose.....	10
Scope and Methodology .....	10

---

## OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

### CAMPUS

Information Technology .....	14
------------------------------	----

### SAN JOSÉ STATE UNIVERSITY RESEARCH FOUNDATION

Property and Equipment .....	15
Trusts and Other Liabilities .....	15
Information Technology .....	17
Password and Data Security .....	17
Equipment Tracking and Security .....	19
Network Security .....	20
Remote Access Security .....	21
User Access Review .....	21
System Backups .....	22

### THE TOWER FOUNDATION

Operating and Administrative Agreements .....	24
Corporate Governance .....	25
Purchasing and Accounts Payable .....	26
Disbursements.....	26
Travel Authorization.....	28
Endowment Administration.....	28
Information Technology .....	29
Password Security.....	29
User Access Review .....	30
Disaster Recovery Plan.....	31

**SPARTAN SHOPS, INC.**

Operational Compliance ..... 33  
    Policies and Procedures ..... 33  
    Risk Management ..... 34  
    Inventory Management ..... 35  
  
Cash Receipts and Handling ..... 36  
  
Petty Cash and Change Funds ..... 37  
  
Fees, Revenues, and Receivables ..... 38  
  
Personnel and Payroll ..... 40  
  
Property and Equipment ..... 41  
  
Information Technology ..... 42  
    Data Security ..... 42  
    User Access Review ..... 43  
    Disaster Recovery Plan ..... 43  
    System Backups ..... 44

**ASSOCIATED STUDENTS SAN JOSÉ STATE UNIVERSITY**

Operating and Administrative Agreements ..... 46  
  
Operational Compliance ..... 46  
  
Segregation of Duties ..... 47  
  
Cash Receipts and Handling ..... 48  
  
Information Technology ..... 50  
    Data Security ..... 50  
    User Access Review ..... 51  
    System Backups ..... 52

**THE STUDENT UNION OF SAN JOSÉ STATE UNIVERSITY**

Fiscal Compliance ..... 53  
  
Cash Receipts and Handling ..... 54  
  
Investments ..... 55

---

CONTENTS

Purchasing and Accounts Payable ..... 56

Property and Equipment ..... 57

Trusts and Other Liabilities ..... 59

Information Technology ..... 60

    Data Security..... 60

    User Access Review ..... 60

    Data Confidentiality Forms ..... 61

    Vendor Service Agreements ..... 62

    Environmental Controls ..... 64

## **APPENDICES**

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

---

## **ABBREVIATIONS**

AS	Associated Students San José State University
AORMA	Auxiliary Organizations Risk Management Authority
ATM	Automated Teller Machine
COO	Chief Operating Officer
CSU	California State University
CSURMA	California State University Risk Management Authority
DMZ	Demilitarized Zone
DRP	Disaster Recovery Plan
EO	Executive Order
ERP	Enterprise Resource Planning
Foundation	San José State University Research Foundation
IT	Information Technology
MOU	Memorandum of Understanding
POS	Point of Sale
RFIN	Resolution of the Committee on Finance
Shops	Spartan Shops, Inc.
SJSU	San José State University
Telnet	Telecommunication Network
TF	The Tower Foundation
UA	University Advancement
Union	The Student Union of San José State University

---

## 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 José State University (SJSU) 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 SJSU campus and its auxiliary organizations from April 5, 2010, through May 14, 2010, and made a study and evaluation of the system of internal compliance/internal control in effect as of May 14, 2010. This report represents our triennial review.

Our study and evaluation at the *San José State University Research Foundation* disclosed conditions that, in our opinion, if not corrected would result in significant errors and irregularities. Specifically, the auxiliary did not maintain adequate internal control over information technology (IT). These conditions, along with other weaknesses, are described in the executive summary and in the body of the report. In our opinion, due to the effect of the weaknesses described above, accounting and administrative control in effect as of May 14, 2010, taken as a whole, was not sufficient to meet the objectives stated above.

Our study and evaluation at *The Tower Foundation* disclosed conditions that, in our opinion, if not corrected would result in significant errors and irregularities. Specifically, the auxiliary did not maintain adequate internal control over purchasing and accounts payable 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, due to the effect of the weaknesses described above, accounting and

administrative control in effect as of May 14, 2010, taken as a whole, was not sufficient to meet the objectives stated above.

Our study and evaluation at *Spartan Shops, Inc.* disclosed conditions that, in our opinion, if not corrected would result in significant errors and irregularities. Specifically, the auxiliary did not maintain adequate internal control over operational compliance 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, due to the effect of the weaknesses described above, accounting and administrative control in effect as of May 14, 2010, taken as a whole, was not sufficient to meet the objectives stated above.

Our study and evaluation at *Associated Students San José State University* disclosed conditions that, in our opinion, if not corrected would result in significant errors and irregularities. Specifically, the auxiliary did not maintain adequate internal control over information technology. These conditions, along with other weaknesses, are described in the executive summary and in the body of the report. In our opinion, due to the effect of the weaknesses described above, accounting and administrative control in effect as of May 14, 2010, taken as a whole, was not sufficient to meet the objectives stated above.

Our study and evaluation at *The Student Union of San José State University* disclosed conditions that, in our opinion, if not corrected would result in significant errors and irregularities. Specifically, the auxiliary did not maintain adequate internal control over information technology. These conditions, along with other weaknesses, are described in the executive summary and in the body of the report. In our opinion, due to the effect of the weaknesses described above, accounting and administrative control in effect as of May 14, 2010, taken as a whole, was not sufficient to meet the objectives stated above.

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

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

## **CAMPUS**

### **INFORMATION TECHNOLOGY [14]**

Auxiliary organization personnel at the San José State University Research Foundation, Spartan Shops, Inc., Associated Students San José State University, and The Student Union of San José State University with access to critical systems or protected data were not always required to complete information security awareness training.

## **SAN JOSÉ STATE UNIVERSITY RESEARCH FOUNDATION**

### **PROPERTY AND EQUIPMENT [15]**

The San José State University Research Foundation (Foundation) did not document its management review of the annual physical inventory.

### **TRUSTS AND OTHER LIABILITIES [15]**

Certain campus program revenues may be inappropriately deposited to, and held in custody by, the Foundation, and trust account agreements could not be provided for all campus programs and projects accounts reviewed.

### **INFORMATION TECHNOLOGY [17]**

Password controls and data security were not always adequate for Foundation systems. Also, the Foundation did not ensure adequate security over computing equipment (computers, servers, etc.) obtained from grant funding that may have contained protected information, and it failed to track these assets in conjunction with its physical inventory count procedures. The internal Foundation network, which stored critical systems with unencrypted protected data, was not properly segmented behind a demilitarized zone to logically separate it from Internet-accessible devices (web servers) also stored on the same network segment. Further, remote access to the Foundation accounting system server was not secure, and the Foundation did not perform a periodic, documented management review of user access privileges within all critical systems and applications containing protected data. In addition, daily and weekly backups for Foundation systems with protected data were not encrypted when stored locally or when in transit to and stored at the off-site storage facility operated by a third-party vendor.

## **THE TOWER FOUNDATION**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS [24]**

The service agreement between The Tower Foundation (TF) and a third-party financial and administrative service provider did not include an appropriate indemnification provision and a right-to-audit clause.

### **CORPORATE GOVERNANCE [25]**

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

## **PURCHASING AND ACCOUNTS PAYABLE [26]**

Certain TF cash disbursements were not appropriately authorized and/or supported by sufficient and appropriate documentation. Further, the TF travel policy did not require documented travel approval prior to domestic business travel.

## **ENDOWMENT ADMINISTRATION [28]**

The TF did not always delineate endowment administrative fees to donors.

## **INFORMATION TECHNOLOGY [29]**

Password and login controls were not always adequate for TF systems, and the TF did not perform a periodic, documented management review of user access privileges within all critical systems and applications containing protected data. Further, the SJSU disaster recovery plan (DRP), which was acknowledged to cover the university advancement (UA) and TF systems, did not reference any specific systems, and therefore did not reflect the criticality and order of priority for SJSU and SJSU-supported systems (including UA/TF servers).

## **SPARTAN SHOPS, INC.**

### **OPERATIONAL COMPLIANCE [33]**

Spartan Shops, Inc. (Shops) had not developed written policies and procedures to address the operation and administration of the Gold Points program, nor had it developed a written risk management policy. In addition, Shops merchandise perpetual inventory records did not always agree with stock on hand, and merchandise price-change procedures did not include a documented management review of price-change reports.

### **CASH RECEIPTS AND HANDLING [36]**

Shops did not document investigations of cash shortages/overages, the check receipt log was not kept current, and bank reconciliations had not been performed since December 2009.

### **PETTY CASH AND CHANGE FUNDS [37]**

Shops had not developed written policies and procedures for periodic, independent cash counts of petty cash and had not performed independent cash counts of either petty cash or cash vault funds in the past three fiscal years.

### **FEES, REVENUES, AND RECEIVABLES [38]**

Point-of-Sale cash transactions from Shops bookstore and dining service operations were erroneously recorded as accounts receivable in the accounting system.

## **PERSONNEL AND PAYROLL [40]**

Employee requests for vacation time off were not always properly supported and approved at Shops.

## **PROPERTY AND EQUIPMENT [41]**

Shops had not performed an independent physical inventory of all property and equipment during the past three years.

## **INFORMATION TECHNOLOGY [42]**

Protected and/or sensitive data was not encrypted when stored in the Shops accounting and payroll systems, and Shops did not perform a periodic, documented management review of user access privileges within all critical systems and applications containing protected data. Further, the Shops IT DRP, dated February 2008, had not been updated to include all systems currently employed by Shops. In addition, daily and weekly backups for Shops systems with protected data were not encrypted when stored locally or when in transit to and stored at alternative storage sites on campus.

## **ASSOCIATED STUDENTS SAN JOSÉ STATE UNIVERSITY**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS [46]**

The operating agreement between the Associated Students San José State University (AS) and the California State University Trustees expired on December 31, 2007, and had not been renewed.

### **OPERATIONAL COMPLIANCE [46]**

AS had not developed a comprehensive written risk management policy.

### **SEGREGATION OF DUTIES [47]**

Certain duties and responsibilities related to payroll processing were not adequately segregated at AS.

### **CASH RECEIPTS AND HANDLING [48]**

Accountability for cash receipts at the AS Print Shop was not always localized to a specific employee, daily cash register opening and closing procedures did not include independent cash counts, and access to the safe was not adequately controlled.

### **INFORMATION TECHNOLOGY [50]**

Protected and/or sensitive data was not encrypted when stored in the AS accounting, payroll, and human resources systems. This is a repeat finding from the prior Auxiliary Organizations audit. Further, AS did not perform a periodic, documented management review of user access privileges within all critical

systems and applications containing protected data. In addition, daily and weekly backups for AS systems with protected data were not encrypted when stored locally or when in transit to and stored at alternative storage sites on campus.

## **THE STUDENT UNION OF SAN JOSÉ STATE UNIVERSITY**

### **FISCAL COMPLIANCE [53]**

The Student Union of San José State University (Union) had not updated its written reserve policy and procedures to reflect current practice.

### **CASH RECEIPTS AND HANDLING [54]**

Administration of cash receipts at the Union did not ensure adequate control at the Event Center box office, and written policies and procedures to address cash shortages/overages had not been developed.

### **INVESTMENTS [55]**

Signature authorization for Union investment accounts was not updated to reflect a change in the chair of the board of directors. This is a repeat finding from a prior Auxiliary Organizations audit.

### **PURCHASING AND ACCOUNTS PAYABLE [56]**

Certain Union credit card purchases were not supported by sufficient and appropriate documentation or reconciled to travel expense claim forms. Further, they were not submitted in a timely manner to accounts payable for reconciliation to credit card statements.

### **PROPERTY AND EQUIPMENT [57]**

The Union had not developed written policies and procedures to address completion of annual physical inventory counts, and adequate documentation was not maintained to show evidence of timely completion of the annual physical inventory.

### **TRUSTS AND OTHER LIABILITIES [59]**

Funds held and administered by the Union on behalf of club sports were not supported by specific written agreements for each account.

### **INFORMATION TECHNOLOGY [60]**

Protected and/or sensitive data was not encrypted when stored in the Union accounting, payroll, and human resources systems, and the Union did not perform a periodic, documented management review of user access privileges within all critical systems and applications containing protected data. Further, Union personnel with access to critical systems or protected data were not required to complete data

confidentiality forms, and certain business arrangements between the Union and third-party systems vendors were not supported by complete and/or written agreements. In addition, the Union's server rooms located in the Student Union and Event Center lacked smoke-detection devices.

---

## 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.

San José State University Research Foundation (Foundation) was established in 1932 as a non-profit public benefit corporation for the purpose of enabling and promoting externally funded programs that further SJSU's comprehensive educational mission. The Foundation manages all externally funded grant and contract activity, including pre- and post- activities; operates and manages business incubators; and provides administrative management services for university programs that are self-supported. These self-supported programs, formerly referred to as "campus programs," are discretionary in nature and include faculty-hosted seminars, conferences, and workshops; faculty-developed specialized training;

construction and renovation projects; and special events. The Foundation is governed by a board of directors comprised of university administrators, faculty, students, and community members.

The Tower Foundation (TF) was established in 2004 as a non-profit public benefit corporation dedicated solely to philanthropy and assisting with the development, investment, administration, and banking of all SJSU philanthropic donations. The TF also aims to grow the university's endowment through donations, bequests, and prudent investment management, including real estate investment transactions. The TF is governed by a board of directors comprised of community members, university administrators, faculty members, alumni, and a student representative. The TF has a total of 3.1 full-time employee positions and relies on the university advancement office and a third-party service provider for administrative and accounting support services.

Spartan Shops, Inc. (Shops) was established in 1956 as a non-profit public benefit corporation to provide bookstore, dining, real estate, information technology services, and other commercial services on the SJSU campus. Shops currently owns and operates the main campus bookstore, as well as several dining establishments and convenience stores on campus. In addition, Shops operates several national-brand restaurants, university residential dining services, and other commercial services, including on-campus catering. Shops' real estate division has been directed to develop, oversee, and coordinate a strategy for real estate development and management and is responsible for the development of faculty and staff housing opportunities in both the rental and ownership markets. Shops' information services division provides technology services, including high-speed Internet, telephone, and cable television for other Shops divisions and for on-campus residents. Shops is governed by a board of directors comprised of university administrators, faculty members, student representatives, and a community member.

Associated Students San José State University (AS) was established in 1980 as a non-profit public benefit corporation to provide for student self-government and to provide services and programs that maximize student life and improve student experiences at SJSU. AS operates the Child Development Center, the Caesar Chavez Community Action Center, Transportation Solutions, the A.S. Print Shop, and the A.S. Computer Services Center. The A.S. General Services Center provides services for students, including check-cashing, money order, notary, and fax services; special events coordination; student organization accounting; legal counseling; and student health insurance programs. Further, AS provides various recreational programs, activities, and services. AS is governed by a board of directors comprised of 13 voting student members and a chairperson.

The Student Union of San José State University (Union) was established in 1982 as a non-profit public benefit corporation to offer quality services and programs that facilitate and enhance the SJSU learning experience and promote social, recreational, cultural, and educational development to the campus community. The Union manages and maintains three major facilities at SJSU -- the Student Union building, the Aquatic Center, and the Event Center -- as well as an ATM kiosk. The Union also administers student body organization programs and instructionally related programs and activities, including a physical fitness center, club sports and fitness programs, and event management. The Union is governed by a board of directors comprised of university administrators, faculty members, student representatives, and a community member.

## **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 May 14, 2010. 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 José State University Research Foundation.

- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Auxiliary Programs
- ▶ Information Technology

The Tower Foundation

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

Spartan Shops, Inc.

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

Associated Students San José 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
- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Auxiliary Programs
- ▶ Information Technology

The Student Union of San José State University

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

The Student Union of San José State University (cont.)

- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Auxiliary Programs
- ▶ Information Technology

Campus

Campus Oversight and Control

We have not performed any auditing procedures beyond May 14, 2010. Accordingly, our comments are based on our knowledge as of that date. Since the purpose of our comments is to suggest areas for improvement, comments on favorable matters are not addressed.

---

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

### **CAMPUS**

#### **INFORMATION TECHNOLOGY**

Auxiliary organization personnel at the San José State University Research Foundation, Spartan Shops, Inc., Associated Students San José State University, and The Student Union of San José State University with access to critical systems or protected data were not always required to complete information security awareness training.

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

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 information security awareness training for all employees with access to critical systems or protected data.

The executive management of each auxiliary stated that management was unaware of the need to conduct training 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, which increases auxiliary and campus exposure to security breaches and could compromise compliance with statutory information security requirements.

#### **Recommendation 1**

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

#### **Campus Response**

We concur. We will develop and implement an action plan for providing information security awareness training to all auxiliary employees with access to critical systems or protected data.

Expected completion date: By the end of January 2011

## **SAN JOSÉ STATE UNIVERSITY RESEARCH FOUNDATION**

### **PROPERTY AND EQUIPMENT**

The San José State University Research Foundation (Foundation) did not document its management review of the annual physical inventory.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the California State University (CSU) system. Section 8.9.7, *Property and Equipment*, states that the auxiliary should reconcile physical inventories to the general ledger on a timely basis with review by management.

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

The Foundation controller stated that not documenting management review of the annual physical inventory was due to oversight.

Failure to document management's review of the annual physical inventory increases the risk that property value may be misrepresented in the financial statements.

#### **Recommendation 2**

We recommend that the Foundation document its management review of the annual physical inventory.

#### **Campus Response**

We concur. We will document the management review of the annual physical inventory.

Expected completion date: By the end of February 2011

### **TRUSTS AND OTHER LIABILITIES**

Certain campus program revenues may be inappropriately deposited to, and held in custody by, the Foundation, and trust account agreements could not be provided for all campus programs and projects accounts reviewed.

The Foundation interim report as of February 28, 2010, indicated that the Foundation administered and maintained 460 campus programs and projects accounts totaling \$10,501,059. We reviewed 39 of these accounts for which trust account agreements or other detailed explanations were available and found that state/campus operating revenue funds totaling \$1,744,487 may be inappropriately held by the Foundation in 16 of the 39 accounts reviewed. We also found that trust account agreements detailing the purpose of the account and required approvals could not be provided for 10 of the 39 accounts.

Each CSU campus shall administer their General and non-General Fund receipts to ensure that the funds are held in proper accounts. Auxiliaries may not accept state funds with the intent of administering them as an agent of the university unless the auxiliaries have been specifically authorized in writing to do so by the university presidents or his/her designee. Said authorization shall be granted judiciously and only when it is advantageous to the university and supportive of the university mission. Such advantages must be clearly documented in writing – mere convenience is not an acceptable advantage. Payment for services is the only instance where state funds may be accepted into an auxiliary organization’s account.

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 written agreements.

The Foundation controller stated that all campus expenditures have been properly reimbursed to the campus. He added that since the two accounts cited fund programs that offer university credit to San José State University (SJSU) students, he agreed that the accounts should be operated and managed by the campus. The Foundation controller also stated that some of the accounts without trust account agreements were established more than ten years ago and the missing agreements were due to oversight.

The campus’ required oversight of state funds is limited when funds are deposited outside the custody of the chief financial officer, while the absence of trust account agreements increases the risk of misunderstandings and miscommunication regarding rights and responsibilities and subjects the auxiliary to potential liability.

### **Recommendation 3**

We recommend that the Foundation:

- a. Complete a review of all campus programs and projects accounts and determine, within 60 days, which accounts contain state/campus operating funds.
- b. Certify that none of the following specific and similar monies reside in Foundation accounts:

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

### **Campus Response**

We concur. We will complete a review of all campus programs and projects and provide certification as required above and by EO 1052 by the deadline given in EO 1052.

## **INFORMATION TECHNOLOGY**

### **PASSWORD AND DATA SECURITY**

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

We found that:

- ▶ Password security parameters were inadequate for the payroll system, as the minimum password length was four characters and there were no complexity requirements, no password expiration, no restrictions for reuse of passwords or access after repeated failed attempts, and no automatic sign-off of users after a period of no use.
- ▶ Protected and/or sensitive data was not encrypted when stored in the accounting and payroll systems. This is a repeat finding from the prior Auxiliary Organizations audit.

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

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

The Foundation information technology (IT) manager stated that the default password security settings of the previous payroll software were determined by the vendor, which the Foundation could not change. He added that the software had been discontinued as of December 31, 2008, and the replacement payroll software has strong password settings. He further stated that lack of encryption in the accounting and payroll systems was due to historical security limitations in these systems and that security improvements from the vendors only recently became available.

Inadequate password and login parameters may compromise the authentication credentials of user account privileges that are embedded into applications and operating systems, which in turn increases the risk of unauthorized access to auxiliary systems and confidential data. Failure to encrypt protected and/or sensitive data could require the auxiliary to notify all affected parties in the event of a breach of security and potentially damage the auxiliary's reputation.

#### **Recommendation 4**

We recommend that the Foundation:

- a. Set effective password and login security parameters for the payroll system in accordance with leading information security industry guidelines and perform an assessment of password security parameters for all other Foundation systems.
- b. Apply encryption controls to the accounting and payroll systems and all other Foundation systems, computers, databases, and file servers that house protected and/or sensitive data.

### **Campus Response**

We concur. We will complete remedial action, by the end of February 2011, to:

- a. Set effective password and login security parameters for the payroll system in accordance with leading information security industry guidelines and perform an assessment of password security parameters for all other Foundation systems.
- b. Apply encryption controls to the accounting and payroll systems and all other Foundation systems, computers, databases, and file servers that house protected and/or sensitive data.

### **EQUIPMENT TRACKING AND SECURITY**

The Foundation did not ensure adequate security over computing equipment (computers, servers, etc.) obtained from grant funding that may have contained protected information and failed to track these assets in conjunction with its physical inventory count procedures.

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

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

The Foundation IT manager stated that at the time the Foundation tracked only centrally managed computing equipment and oversaw procurement of grant computing equipment, but did not monitor that equipment for adequate security because the equipment was not at its location and was operated by campus academic personnel that do not report to the Foundation.

Inadequate security and accountability of computing equipment, especially that containing personal confidential information or with accessibility to such protected information, increases the risk of loss and inappropriate use of auxiliary resources and increases exposure to information security breaches.

### **Recommendation 5**

We recommend that the Foundation ensure the security of and maintain an inventory of all computing equipment purchased by the Foundation, including those purchased via grant funding.

### **Campus Response**

We concur. We will ensure the security of and maintain an inventory of all computing equipment purchased by the Foundation, including those purchased via grant funding.

Expected completion date: By the end of March 2011

### **NETWORK SECURITY**

The internal Foundation network, which stored critical systems with unencrypted protected data, was not properly segmented behind a demilitarized zone (DMZ) to logically separate it from Internet-accessible devices (web servers) also stored on the same network segment.

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

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates network segmentation via a DMZ to logically separate any protected data residing on internal auxiliary systems from Internet-accessible devices.

The Foundation IT manager stated that the Foundation had considered the need for a DMZ but found that the firewall rules required would have added additional complexities during a time of resource constraints and other IT priorities.

The lack of a DMZ to separate and protect internal Foundation resources from Internet-accessible devices increases the risk of internal network exposure to security compromises and inadequate security over information assets with protected data.

### **Recommendation 6**

We recommend that the Foundation perform an assessment and evaluate the feasibility of implementing a DMZ to separate and protect internal Foundation resources from Internet-accessible devices.

### **Campus Response**

We concur. We will perform an assessment and evaluate the feasibility of implementing a DMZ to separate and protect internal Foundation resources from Internet-accessible devices.

Expected completion date: By the end of March 2011

## **REMOTE ACCESS SECURITY**

Remote access to the Foundation accounting system server was not secure.

We found that Telecommunication Network (Telnet), an unsecure remote access protocol that allows users to connect to remote computers and transmits data in clear text, was enabled to permit remote access by the Foundation.

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 securing remote access to auxiliary systems.

The Foundation IT manager stated that at the time remote access was first implemented on this system, Telnet provided the best network compatibility and was considered adequate.

Failure to properly secure remote access to auxiliary servers increases the risk that an attacker who is able to monitor network traffic could capture sensitive information or authentication credentials and, therefore, gain access to network resources and exploit vulnerabilities. This could lead to the loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

### **Recommendation 7**

We recommend that the Foundation replace Telnet remote access with a more secure remote access protocol (such as Secure Shell) or enforce internal firewall restrictions on Telnet such that it could only be accessed once a virtual private network connection has been established.

### **Campus Response**

We concur. We will either replace Telnet remote access with a more secure remote access protocol (such as Secure Shell) or enforce internal firewall restrictions on Telnet such that it could only be accessed once a virtual private network connection has been established.

Expected completion date: By the end of February 2011

## **USER ACCESS REVIEW**

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

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

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

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

The Foundation IT manager stated that he was unaware of the requirement to perform periodic, documented management reviews of user access privileges within Foundation systems, but he added that user access was reviewed on an event basis such as employee separation or job responsibility change.

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

### **Recommendation 8**

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

### **Campus Response**

We concur. We will implement procedures to conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually.

Expected completion date: By the end of March 2011

### **SYSTEM BACKUPS**

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

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

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

The Foundation IT manager stated that he was unaware of this requirement and was not certain if the backup systems currently used by the Foundation included the capability to encrypt data.

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

#### **Recommendation 9**

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

#### **Campus Response**

We concur. We will encrypt system backups of protected data and ensure that the off-site transfer and storage of backups is secure.

Expected completion date: By the end of February 2011

## **THE TOWER FOUNDATION**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS**

The service agreement between The Tower Foundation (TF) and a third-party financial and administrative service provider did not include an appropriate indemnification provision and a right-to-audit clause.

We found that the indemnification provision in the financial and administrative service provider agreement did not indemnify the CSU Trustees, the campus, and the State of California. In addition, the agreement did not contain a right-to-audit clause.

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

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

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that business arrangements be supported by complete, written agreements that are executed in a timely manner and include appropriate indemnification and right-to-audit clauses.

The TF chief operating officer (COO) and associate vice president of advancement operations stated that although certain documented clauses within the current agreement could be strengthened, all parties involved in the agreement had a clear understanding of their roles and responsibilities.

The absence of an appropriate indemnification provision and a right-to-audit clause increases the risk of misunderstandings and miscommunication regarding rights and responsibilities and subjects the auxiliary and CSU to potential liability.

### **Recommendation 10**

We recommend that the TF:

- a. Amend the cited agreement with an appropriate indemnification and right-to-audit clause.
- b. Ensure that all future agreements with third parties include an appropriate indemnification provision and a right-to-audit clause.

### **Campus Response**

We concur. We implemented the compliance action in May 2010 to:

- a. Amend the cited agreement with an appropriate indemnification and right-to-audit clause.
- b. Ensure that all future agreements with third parties include an appropriate indemnification provision and a right-to-audit clause.

## **CORPORATE GOVERNANCE**

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

We found amendments to the Bylaws made on April 10, 2006, and September 11, 2007, that had not been filed with the chancellor's office.

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

The TF COO and associate vice president of advancement operations stated that the auxiliary operated under the assertion that only substantial changes to the Bylaws should be submitted to the chancellor's office.

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

### **Recommendation 11**

We recommend that the TF promptly file the cited amendments with the Financing and Treasury department at the Office of the Chancellor and ensure that all future changes/amendments to Bylaws are filed within 30 calendar days.

### **Campus Response**

We concur. We filed the cited amendments with the Financing and Treasury department at the Office of the Chancellor in May 2010 and have issued a management reminder to ensure that all future changes/amendments to Bylaws are filed within 30 calendar days.

## **PURCHASING AND ACCOUNTS PAYABLE**

### **DISBURSEMENTS**

Certain TF cash disbursements were not appropriately authorized and/or supported by sufficient and appropriate documentation.

We reviewed 28 cash disbursements and two travel reimbursements and found that:

- ▶ One of 24 checks over \$5,000 was not signed by two individuals.
- ▶ One of the two travel reimbursements for club sports airfare travel was not supported by air travel release forms or signed waivers from the 20 students traveling by air on campus-program-sponsored trips.
- ▶ In one of two instances where competitive bidding was required, price quotes from three or more vendors were not obtained, and documentation of the reason quotes were not obtained was not on file.

SJSU TF, *Banking: Authority and Responsibility Policy*, dated March 10, 2007, states that for checks over \$5,000, two signatures are required. One of these signatures may be stamped, but one must be manual.

EO 590, *California State University Systemwide Student Air Travel Policy*, dated March 26, 1992, and its successor, EO 1041, *California State University Student Travel Policy*, dated July 1, 2009, state that all students participating in CSU-affiliated programs that require air travel shall be required to acknowledge that they have been informed of the risks of air travel required by such programs and to sign a statement certifying that they have been informed of and undertake such air travel voluntarily with full knowledge of such risks, and release and hold harmless the State of California, the CSU, the campus affiliated with the program requiring air travel, and each and every officer, agent, and employee of each of them, from any and all claims and causes of action that the student, or any person(s) claiming through the student, may have against any of the above institutions or persons, by reason of any accident, illness or injuries, death, or other consequences resulting directly or indirectly from or in any manner arising out of, or in connection with, the student being a passenger on a flight.

SJSU Tower Foundation *Procurement Policy*, dated February 1, 2008, requires that price quotes from three or more vendors be obtained either in writing or by phone. If quotes were not obtained, there must be documentation explaining why they were not acquired.

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

The TF controller stated that the failure to obtain a signature for the check over \$5,000 was due to oversight, and the failure to ensure that student travel is supported by signed waivers or release forms was due to a lack of awareness of the requirement among many on campus. She further stated that the lack of evidence of competitive bidding was due to oversight.

The lack of appropriate authorization and/or sufficient and appropriate supporting documentation increases the risk of errors, irregularities, and misappropriation of funds, while the lack of release forms or signed waivers for students' traveling by air on campus-program-sponsored trips increases the risk of legal liability.

### **Recommendation 12**

We recommend that the TF:

- a. Obtain two signatures on all checks over \$5,000, as required by TF policy.
- b. Obtain signed release forms/waivers from each student traveling by air on campus-program-sponsored trips.
- c. Reiterate to staff existing procurement policy regarding competitive bidding.

### **Campus Response**

We concur. We will implement procedures to effectuate remedial actions, by the end of February 2011, to:

- a. Obtain two signatures on all checks over \$5,000, as required by TF policy.
- b. Obtain signed release forms/waivers from each student traveling by air on campus-program-sponsored trips.
- c. Reiterate to staff existing procurement policy regarding competitive bidding.

## TRAVEL AUTHORIZATION

The TF travel policy did not require documented travel approval prior to domestic business travel.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system.

Section 8.9.1, *Cash*, states that the auxiliary should disburse cash in a consistent manner utilizing systems that ensure integrity of existing controls, with annual management review.

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

The TF controller stated that the travel policy did not require prior approval for domestic business travel; however, it was a practice to require a copy of the provost's approval prior to processing travel advances and reimbursements for international travel.

Failure to sufficiently document travel approval increases the risk of errors, irregularities, and misappropriation of funds.

### Recommendation 13

We recommend that the TF revise its travel policy to require completion of travel request forms prior to travel and ensure that the travel requests are properly reviewed and approved.

### Campus Response

We concur. We will revise the travel policy to require completion of travel request forms prior to travel and ensure that the travel requests are properly reviewed and approved.

Expected completion date: By the end of January 2011

## ENDOWMENT ADMINISTRATION

The TF did not always delineate endowment administrative fees to donors.

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 TF COO and associate vice president of advancement operations stated that the endowment agreements referred to the TF investment policy, which delineates the management fees, but the fees were not specifically outlined in old endowment agreements. She further stated that donors received an annual communication that notates the fee, but it was not specifically meant to notify the donors of such fees.

Failure to delineate management fees within the endowment agreement and to notify all donors of such fees increases auxiliary exposure to liability.

#### **Recommendation 14**

We recommend that the TF update its endowment agreement to specifically address the TF's administrative fees and ensure that all donors are notified of the administrative fees.

#### **Campus Response**

We concur. We updated the endowment agreement template to specifically address the TF's administrative fees in October 2010 and have issued a management reminder to ensure that all donors are notified of the administrative fees.

## **INFORMATION TECHNOLOGY**

### **PASSWORD SECURITY**

Password and login controls were not always adequate for TF systems.

We found that:

- ▶ The password and login parameters for the accounting system did not enforce any minimum password length, password complexity, periodic expiration, or login security.
- ▶ The password and login parameters for the donor system only enforced a minimum length of 6 characters, and there was no password expiration.

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 TF COO and associate vice president of advancement operations stated that the accounting system was hosted offsite by a third-party vendor, and she was unaware of whether different settings could be implemented. She further stated that the accounting system recommended 90-day password expiration and sent a reminder to users, but enforcement was not enabled. Finally, she stated that the donor system password controls were the default settings, and she was unaware of whether different settings could be implemented.

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

### **Recommendation 15**

We recommend that the TF set effective password and login security parameters for the accounting and donor systems in accordance with leading information security industry guidelines and perform an assessment of password security parameters for all other TF systems.

### **Campus Response**

We concur. We will set effective password and login security parameters for the accounting and donor systems in accordance with leading information security industry guidelines and perform an assessment of password security parameters for all other TF systems.

Expected completion date: By the end of January 2011

### **USER ACCESS REVIEW**

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

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

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

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

The TF COO and associate vice president of advancement operations stated that she was unaware of the requirement to perform periodic, documented management reviews of user access privileges within TF systems, but she added that user access was informally reviewed upon employee separation or job responsibility change.

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

#### **Recommendation 16**

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

#### **Campus Response**

We concur. We will implement procedures to conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually.

Expected completion date: By the end of February 2011

#### **DISASTER RECOVERY PLAN**

The SJSU disaster recovery plan (DRP), which was acknowledged to cover the university advancement (UA) and TF systems, did not reference any specific systems and, therefore, did not reflect the criticality and order of priority for SJSU and SJSU-supported systems (including UA/TF servers).

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

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

The TF COO and associate vice president of advancement operations stated that UA/TF systems were managed by the SJSU IT department and were therefore thought to have been sufficiently documented within the SJSU DRP.

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

**Recommendation 17**

We recommend that the campus and TF collaborate to complete a comprehensive IT DRP that includes all critical systems.

**Campus Response**

We concur. We will design a comprehensive IT DRP that includes all critical systems.

Expected completion date: By the end of March 2011

## **SPARTAN SHOPS, INC.**

### **OPERATIONAL COMPLIANCE**

#### **POLICIES AND PROCEDURES**

Spartan Shops, Inc. (Shops) had not developed written policies and procedures to address the operation and administration of the Gold Points program.

Gold Points are pre-deposited dollars held in an individual account. The account holder can access the dollars with an SJSU ID or VIP Gold Card, and the money can be used to purchase goods and services on the SJSU campus. Specifically, we found that policies and procedures had not been developed to address:

- ▶ Recording and administration of Gold Points subsequent to the deposit of funds by students.
- ▶ Administration of outstanding and idle Gold Points for students no longer enrolled at the university.

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 operation and administration of prepaid points programs.

The Shops executive director stated that Shops had not created a written policy for the operation and administration of Gold Points due to management oversight.

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

#### **Recommendation 18**

We recommend that Shops develop written policies and procedures to address the operation and administration of the Gold Points program, including recording and administration of Gold Points subsequent to the deposit of funds by students and the administration of outstanding/idle Gold Points for students no longer enrolled at the university.

#### **Campus Response**

We concur. We will develop written policies and procedures to address the operation and administration of the Gold Points program, including recording and administration of Gold Points

subsequent to the deposit of funds by students and the administration of outstanding/idle Gold Points for students no longer enrolled at the university.

Expected completion date: By the end of February 2011

## **RISK MANAGEMENT**

Shops had not developed a written risk management policy.

We found that Shops 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 implement a risk mitigation program that coordinates with the campus' risk assessment and mitigation plan.

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

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.7, *Risk Management*, states that auxiliary organizations should develop programs to manage risk related to activities in which the organizations are engaged.

The Shops executive director stated that the auxiliary addressed risk management in its insurance policy. He further stated that the auxiliary was unaware of the requirement for a separate risk management policy.

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

### **Recommendation 19**

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

### **Campus Response**

We concur. We will develop and adopt a written risk management policy, including procedures to actively identify, analyze, quantify, and manage risk.

Expected completion date: By the end of March 2011

## **INVENTORY MANAGEMENT**

Shops merchandise perpetual inventory records did not always agree with stock on hand, and merchandise price-change procedures did not include a documented management review of price-change reports.

We found that:

- ▶ Discrepancies existed between merchandise perpetual inventory records and stock on hand. Two of eleven inventory classes we reviewed disclosed inventory shortages totaling \$995 between perpetual inventory records and stock on hand.
- ▶ Merchandise price-change procedures did not include a documented management review of merchandise price-change reports to ensure there were no inappropriate or unauthorized price changes.

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 merchandise perpetual inventory records and price changes.

The Shops executive director stated that the lack of sufficient inventory management controls was due to the recent implementation of an enterprise resource planning (ERP) system, Epicor.

Insufficient administration of merchandise perpetual inventory records and price changes increases the risk of loss or misappropriation of goods and errors and irregularities in merchandise pricing.

### **Recommendation 20**

We recommend that Shops:

- a. Review and revise its inventory management controls to ensure the accuracy of merchandise perpetual inventory records.
- b. Perform documented management reviews of merchandise price changes on a routine basis, such as monthly.

### **Campus Response**

We concur. We will implement management procedures to effectuate compliance action, by the end of February 2011, to:

- a. Review and revise the inventory management controls to ensure the accuracy of merchandise perpetual inventory records.
- b. Perform documented management reviews of merchandise price changes on a routine basis, such as monthly.

## CASH RECEIPTS AND HANDLING

Shops did not document investigations of cash shortages/overages, the check receipt log was not kept current, and bank reconciliations had not been performed since December 2009.

We found that:

- ▶ Investigations of cash shortages/overages were not documented, and Shops' cash-handling policy did not require documentation of overage/shortage reviews.
- ▶ Checks had not been recorded in the check receipt log since February 2010, a two-month delay at the time of our review.
- ▶ Bank reconciliations had not been performed since December 2009, a four-month delay at the time of our review.

The Shops *Cash Handling Policy* states that all overages/shortages exceeding \$5 must be reviewed. Various thresholds per dollar amount are subject to further disciplinary actions.

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

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

Shops executive director stated that the lack of documentation for cash overage/shortage investigations, failure to maintain the check receipt log, and untimely bank reconciliations were all due to a recent decrease in staff size.

Inadequate administration of cash receipts and untimely bank reconciliations increase exposure to loss from inappropriate acts, limit the auxiliary's ability to detect errors and irregularities, and compromise accountability.

### **Recommendation 21**

We recommend that Shops:

- a. Update the Shops' cash shortage policy/procedure to require documentation of investigations and ensure proper documentation of cash shortage and/or overage investigations.
- b. Record checks to the check receipt log in a timely manner.
- c. Perform timely bank reconciliations.

### **Campus Response**

We concur. We will implement management procedures to effectuate compliance action, by the end of January 2011, to:

- a. Update the Shops' cash shortage policy/procedure to require documentation of investigations and ensure proper documentation of cash shortage and/or overage investigations.
- b. Record checks to the check receipt log in a timely manner.
- c. Perform timely bank reconciliations.

## **PETTY CASH AND CHANGE FUNDS**

Shops had not developed written policies and procedures for periodic, independent cash counts of petty cash and had not performed independent cash counts of either petty cash or cash vault funds in the past three fiscal years.

We found that:

- ▶ Written policies and procedures had not been developed for periodic, independent cash counts of petty cash.
- ▶ Independent cash counts of eight petty cash funds totaling \$1,505 and ranging from \$100 to \$320 had not been performed for fiscal years 2006/07, 2007/08, and 2008/09.
- ▶ Independent cash counts of the \$55,000 cash vault fund located in the cashier's office had not been performed for fiscal years 2006/07, 2007/08, and 2008/09.

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 petty cash and cash vault funds, including written policies and procedures and periodic, independent cash counts.

The Shops *Vault Policies* require no less than two random audits per calendar month of the cashier's office vault by an individual who normally works outside of the vault (e.g., the operations manager, textbook manager, or store director). The senior vault cashier will be responsible for ensuring that these audits occur.

The Shops executive director stated that lack of written policies and procedures and periodic, independent cash counts were due to oversight.

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

### **Recommendation 22**

We recommend that Shops:

- a. Develop and implement written policies for periodic, independent cash counts of petty cash.
- b. Perform and document periodic, independent cash counts of all petty cash.
- c. Perform and document independent cash counts of cash vault funds as required by Vault Policies.

### **Campus Response**

We concur. We will implement management procedures to effectuate compliance action, by the end of January 2011, to:

- a. Develop and implement written policies for periodic, independent cash counts of petty cash.
- b. Perform and document periodic, independent cash counts of all petty cash.
- c. Perform and document independent cash counts of cash vault funds as required by Vault Policies.

## **FEES, REVENUES, AND RECEIVABLES**

Point-of-Sale (POS) cash transactions from Shops bookstore and dining service operations were erroneously recorded as accounts receivable in the accounting system.

We reviewed the accounts receivable aging report as of April 15, 2010, and found that POS cash transactions between January 2010 and March 2010 were erroneously recorded and aged as

outstanding accounts receivable. The Shops' POS system was migrated to a new Enterprise Resource Planning (ERP) system in January 2010. The ERP system was designed to initially hold POS transaction scans as accounts receivable. Then when the cashier entered payment for the transaction into the POS, the ERP system was designed to automatically apply the payment to cancel the transaction being held as accounts receivable. However, the ERP system was not functioning as designed and was not automatically applying POS payments to cancel POS transaction scans held within the system as accounts receivable. Therefore, the POS transaction records remained as outstanding accounts receivable from 61 to 90 days in the accounts receivable aging report and required manual correction.

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 8.9.1, *Cash*, states that the auxiliary should receive cash in a consistent manner utilizing systems that ensure integrity of existing internal controls.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.4, *Receivables*, states that the auxiliary should properly record and promptly collect receivables in a consistent manner utilizing systems that ensure integrity of existing internal controls.

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 proper recording of accounting transactions.

The Shops executive director stated that the auxiliary and its ERP system vendor were in the process of evaluating errors and dysfunctions identified in the implementation phase of the new ERP system for corrective action.

Improper recording of accounting transactions increases the risk of misrepresentation in the financial statements.

### **Recommendation 23**

We recommend that Shops complete its evaluation of errors and dysfunctions identified within the new ERP system, including the erroneous accounting of POS cash sales transactions as accounts receivable, and take action for prompt resolution.

### **Campus Response**

We concur. We will complete the evaluation of errors and dysfunctions identified within the new ERP system, including the erroneous accounting of POS cash sales transactions as accounts receivable, and take action for prompt resolution.

Expected completion date: By the end of February 2011

## **PERSONNEL AND PAYROLL**

Employee requests for vacation time off were not always properly supported and approved at Shops.

We reviewed requests for vacation time off for eight employees and found that:

- ▶ In four instances, the required forms requesting vacation time off were not on file.
- ▶ In three instances, neither the employee requesting the vacation time off nor the supervisor approving the vacation time off request form properly completed the form. The forms lacked request and approval dates and a supervisor signature.

The Shops *Employee Handbook, Notification of Absences or Lateness*, states that the employee's immediate supervisor must approve requests for time off for doctor appointments or other time off. Requests for leave of any kind must be submitted in writing to management and should be submitted at the earliest possible date in compliance with the type of leave requested.

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.

The Shops executive director stated that management had lost oversight of ensuring supervisor review and approval of employee requests for vacation time off.

Failure to properly document and approve employee requests for vacation time off increases the risk of errors and irregularities, which may in turn lead to under- or over-compensation of employees and exposure to increased liability for the auxiliary.

### **Recommendation 24**

We recommend that Shops reiterate to all employees the vacation time off request policy requirements to ensure that all requests are documented and approved by management.

### **Campus Response**

We concur. We will reiterate to all employees the vacation time off request policy requirements to ensure that all requests are documented and approved by management.

Expected completion date: By the end of January 2011

## **PROPERTY AND EQUIPMENT**

Shops had not performed an independent physical inventory of all property and equipment during the last three years.

We found that inventory custodians were asked to confirm the property and equipment in their custody; however, there was no independent verification of the confirmations provided by the custodians.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.7, *Property and Equipment*, states that the auxiliary should establish a written system that ensures physical inspection of property and equipment on a service life schedule and reconciliation to the general ledger on a timely basis with review by management.

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

The Shops executive director stated that the failure to perform a periodic, independent physical inventory of property and equipment was due to limited resources and staffing constraints.

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

### **Recommendation 25**

We recommend that Shops perform a periodic, independent physical inventory of its property and equipment, including reconciliation to the general ledger, with review by management.

### **Campus Response**

We concur. We will implement management procedures to perform a periodic, independent physical inventory of property and equipment, including reconciliation to the general ledger, with review by management.

Expected completion date: By the end of February 2011

## **INFORMATION TECHNOLOGY**

### **DATA SECURITY**

Protected and/or sensitive data was not encrypted when stored in the Shops' accounting and payroll systems.

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

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

The Shops director of IT and services stated that the accounting system was not encrypted due to uncertainty of the encryption mechanisms supported by the vendor, and that because the payroll database was under the control of the vendor, Shops had no control over the encryption of data.

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

### **Recommendation 26**

We recommend that Shops apply encryption controls to all Shops systems, computers, databases, and file servers that house protected and/or sensitive data.

### **Campus Response**

We concur. We will apply encryption controls to all Shops systems, computers, databases, and file servers that house protected and/or sensitive data.

Expected completion date: By the end of February 2011

## **USER ACCESS REVIEW**

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

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

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

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

The Shops director of IT and services stated that Shops was unaware of the requirement to perform periodic, documented management reviews of user access privileges within Shops systems.

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

### **Recommendation 27**

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

### **Campus Response**

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

Expected completion date: By the end of February 2011

## **DISASTER RECOVERY PLAN**

The Shops IT DRP, dated February 2008, had not been updated to include all systems currently employed by Shops.

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

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

The Shops director of IT and services stated that a comprehensive IT DRP for all systems managed by the IT department was being developed but was not yet complete due to other priorities.

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

### **Recommendation 28**

We recommend that Shops complete a comprehensive IT DRP that is inclusive of all critical systems.

### **Campus Response**

We concur. We will design a comprehensive IT DRP that is inclusive of all critical systems.

Expected completion date: By the end of March 2011

## **SYSTEM BACKUPS**

Daily and weekly backups for Shops systems with protected data were not encrypted when stored locally or when in transit to and stored at alternative storage sites on campus.

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

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

The Shops director of IT and services stated that it was unknown whether the backup systems used by Shops included the capability to encrypt data.

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

**Recommendation 29**

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

**Campus Response**

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

Expected completion date: By the end of February 2011

## **ASSOCIATED STUDENTS SAN JOSÉ STATE UNIVERSITY**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS**

The operating agreement between the Associated Students San José State University (AS) and the CSU Trustees expired on December 31, 2007, and had not been renewed.

Title 5 §42501 indicates that a written operating agreement on behalf of the State of California by the chancellor of the CSU and the auxiliary organization is required for the performance by such auxiliary organization of any functions listed in §42500.

The AS finance and accounting manager stated that he had been in discussion with university administration regarding the need for a current operating agreement, but university administration had not yet taken action.

The absence of a current, written agreement increases the risk of misunderstandings and miscommunication regarding rights and responsibilities.

#### **Recommendation 30**

We recommend that AS promptly renew its operating agreement with the CSU Trustees and implement a process to ensure that future agreements are renewed in a timely fashion.

#### **Campus Response**

We concur. We will renew the operating agreement with the CSU Trustees and implement a process to ensure that future agreements are renewed in a timely fashion.

Expected completion date: By the end of January 2011

### **OPERATIONAL COMPLIANCE**

AS had not developed a comprehensive 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 implement a risk mitigation program that coordinates with the campus' risk assessment and mitigation plan.

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

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.7, *Risk Management*, states that auxiliary organizations should develop programs to manage risk related to activities in which the organizations are engaged.

The AS finance and accounting manager stated that AS has a number of risk management procedures but was unaware of the requirement for a comprehensive written risk management policy.

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

### **Recommendation 31**

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. We will develop and adopt a written and consolidated risk management policy, including procedures to actively identify, analyze, quantify, and manage risk.

Expected completion date: By the end of February 2011

## **SEGREGATION OF DUTIES**

Certain duties and responsibilities related to payroll processing were not adequately segregated at AS.

We found that one employee with payroll processing responsibilities also had administrative rights in the payroll system. These administrative rights allowed the employee to make payroll changes within the payroll system.

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 internal 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 AS finance and accounting manager stated that he was unaware that this employee had administrative rights to the payroll system and that access was most likely accidentally granted when the new payroll system was recently implemented.

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

### **Recommendation 32**

We recommend that AS revoke administrative rights access to the payroll system for employees with payroll processing duties.

### **Campus Response**

We concur. We will implement procedures to revoke administrative rights access to the payroll system for employees with payroll processing duties.

Expected completion date: By the end of January 2011

## **CASH RECEIPTS AND HANDLING**

Accountability for cash receipts at the AS Print Shop was not always localized to a specific employee, daily cash register opening and closing procedures did not include independent cash counts, and access to the safe was not adequately controlled.

We found that:

- ▶ Separate logons and close-out procedures were not used to localize accountability when multiple cashiers used the same cash register.
- ▶ Daily opening procedures did not include a count of the opening banks for each cash register to verify the beginning amount of cash.
- ▶ Daily close-out procedures did not include an independent count of each cashier's drawer by a supervisor or other staff member. Instead, the last cashier on duty for the day counted cash, prepared a closing worksheet, and dropped the cash in the safe. The supervisor only reviewed the closing worksheet if the worksheet showed a material variance.
- ▶ The safe was located in an unsecure location under one of the cash registers in the middle of the store. In addition, the safe was always unlocked and all employees had access to the safe during business hours.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system.

Section 8.9.1, *Cash*, states that the auxiliary should receive cash in a consistent manner utilizing systems that ensure integrity of existing internal controls.

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

The AS finance and accounting manager stated that because of the high volume and low value of transactions, the cashiering process was controlled by one full-time staff member to minimize staffing costs, which resulted in the lack of localized accountability and independent cash counts during opening and closing procedures. He further stated that the safe was stored in the most convenient location and remained unlocked to allow for more flexibility of the numerous employees that needed to retrieve their cash banks throughout the day.

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

### **Recommendation 33**

We recommend that AS:

- a. Localize accountability over cash receipts when multiple cashiers operate the same register.
- b. Update daily close-out procedures to include an independent count of each cashier's drawer by a supervisor or other staff member.
- c. Update daily opening procedures to include a count of the opening banks for each cash register to verify the beginning amount of cash.
- d. Place the safe in a secure location, keep the safe locked during business hours, and restrict access to the safe to only those employees with a business need for such access.

### **Campus Response**

We concur. We will implement procedures to effectuate compliance actions, by the end of January 2011, to:

- a. Localize accountability over cash receipts when multiple cashiers operate the same register.
- b. Update daily close-out procedures to include an independent count of each cashier's drawer by a supervisor or other staff member.

- c. Update daily opening procedures to include a count of the opening banks for each cash register to verify the beginning amount of cash.
- d. Place the safe in a secure location, keep the safe locked during business hours, and restrict access to the safe to only those employees with a business need for such access.

## **INFORMATION TECHNOLOGY**

### **DATA SECURITY**

Protected and/or sensitive data was not encrypted when stored in the AS accounting, payroll, and human resources systems. This is a repeat finding from the prior Auxiliary Organizations audit.

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

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

The AS IT manager stated that all AS systems were not easily encrypted, but he added that several encryption solutions were being evaluated.

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

#### **Recommendation 34**

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

#### **Campus Response**

We concur. We will design encryption controls to all AS systems, computers, databases, and file servers that house protected and/or sensitive data.

Expected completion date: By the end of February 2011

## **USER ACCESS REVIEW**

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

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

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

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

The AS IT manager stated his belief that due to the limited number of AS personnel with access to financial systems (three accountants and one human resources staff) and the fact that all other users in the organization are set to user level access, this requirement was not deemed necessary for the organization. He added that after further consideration, annual management user access reviews for the few users who have access would be conducted.

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

### **Recommendation 35**

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

### **Campus Response**

We concur. We will implement procedures to conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually.

Expected completion date: By the end of February 2011

## **SYSTEM BACKUPS**

Daily and weekly backups for AS systems with protected data were not encrypted when stored locally or when in transit to and stored at alternative storage sites on campus.

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

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

The AS IT manager stated that AS was unaware of the requirement to encrypt system backups.

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

### **Recommendation 36**

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

### **Campus Response**

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

Expected completion date: By the end of February 2011

## **THE STUDENT UNION OF SAN JOSÉ STATE UNIVERSITY**

### **FISCAL COMPLIANCE**

The Student Union (Union) had not updated its written reserve policy to reflect current practice.

We found that the Chancellor's Office Repair and Replacement Reserve was currently maintained and controlled by the campus.

The Union *Reserve Policies* state that the Chancellor's Office Repair and Replacement Reserves is maintained and controlled by the chancellor's office.

Education Code §89904(b), §89904.5, and §89905 indicate that reserve planning is necessary.

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 8.9.9, *Reserves and Net Assets*, states, in part, that an auxiliary implement financial standards, which will assure fiscal viability, including proper provision for professional management, adequate working capital, adequate reserve funds for current operations and capital replacements, and adequate provisions for new business requirements.

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

The Union associate director of administrative services stated that failure to update the reserve policy was due to oversight.

Failure to ensure that current business practice agrees with written policy increases the risk that inconsistencies and misunderstandings will occur and subjects the Union to potential liability.

#### **Recommendation 37**

We recommend that the Union update its reserve policy to reflect current practice.

#### **Campus Response**

We concur. We will update the reserve policy to reflect current practice.

Expected completion date: By the end of January 2011

## CASH RECEIPTS AND HANDLING

Administration of cash receipts at the Union did not ensure adequate control at the Event Center box office, and written policies and procedures to address cash shortages/overages had not been developed.

We found that:

- ▶ Separate log-on and close-out procedures were not used to localize accountability when multiple cashiers used the same cash register at the Event Center box office.
- ▶ A back-up employee had not been designated for verification and deposit of cash receipts at the Event Center box office.
- ▶ Written policies and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery, had not been developed.

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

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

The Union associate director of administrative services stated that present mitigating controls were considered sufficient for cashiers using the same cash register at the Event Center box office. She further stated that not having a back-up person for verifying and depositing cash receipts at the Event Center box office was due to staff turnover. She also stated that procedures addressing cash shortages and/or overages were incorporated into the daily cash handling procedures in certain individual cash centers but that not all cash centers have specific written procedures.

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

### **Recommendation 38**

We recommend that the Union:

- a. Localize accountability over cash receipts when multiple cashiers operate the same register at the Event Center box office.

- b. Designate back-up personnel for verification and deposit of cash receipts at the Event Center box office.
- c. Establish written policy and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery.

### **Campus Response**

We concur. We will implement procedures to effectuate compliance actions, by the end of February 2011, to:

- a. Localize accountability over cash receipts when multiple cashiers operate the same register at the Event Center box office.
- b. Designate back-up personnel for verification and deposit of cash receipts at the Event Center box office.
- c. Establish written policy and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery.

## **INVESTMENTS**

Signature authorization for Union investment accounts was not updated to reflect a change in the chair of the board of directors. This is a repeat finding from a 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 strong controls over the administration of investment accounts.

The Union associate director of administrative services stated that failure to update the authorized signer was due to oversight.

Failure to update signature authorization increases the risk of errors, irregularities, and misappropriation of funds.

### **Recommendation 39**

We recommend that the Union promptly update the signature authorization for its investment accounts to reflect the change in the chair of the board of directors.

### **Campus Response**

We concur. We will update the signature authorization for investment accounts to reflect the change in the chair of the board of directors.

Expected completion date: By the end of January 2011

## **PURCHASING AND ACCOUNTS PAYABLE**

Certain Union credit card purchases were not supported by sufficient and appropriate documentation, not submitted to accounts payable for reconciliation to credit card statements in a timely manner, and not reconciled to travel expense claim forms.

We reviewed credit card statements from November 2009 to February 2010 and found that:

- ▶ For November 2009, the receipt for one purchase for \$90 was submitted five months after the charge transaction, and 15 travel-related charges totaling \$940 were not reconciled to travel expense claim forms.
- ▶ For January 2010, one purchase for \$473 was not supported by a receipt, and the receipts for four purchases totaling \$3,169 were submitted two months after the charge transactions.
- ▶ For February 2010, 11 purchases totaling \$2,345 were not supported by receipts.

The *Union Credit Card Use Guidelines* state that upon completing a credit card transaction, the card user shall immediately record the transaction on the corporate credit card purchase authorization form. If the card user has lost receipts/invoices and a duplicate copy cannot be obtained from the vendor, the lost/itemized receipt form is completed. All appropriate paperwork, such as purchase orders, receipts/invoices, and other documentation, must be forwarded to accounts payable within three days of purchase. In addition, original itemized receipts and/or appropriate documentation for all travel expenses must be submitted for each charge.

The *Union Accounts Payable Procedure* states that the accounts payable technician reviews and reconciles the pre-paid corporate Visa card prior to month-end close.

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

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

business practices. Sound business practice mandates that all credit card purchases be fully supported, promptly submitted, and properly reconciled.

The Union associate director of administrative services stated that failure to obtain sufficient and appropriate documentation and perform timely and adequate credit card reconciliations was due to utilizing temporary staff when the accounts payable clerk was out on maternity leave.

Insufficient supporting documentation for credit card purchases and untimely and inadequate credit card reconciliations increase the risk of errors, irregularities, and misappropriation of funds.

#### **Recommendation 40**

We recommend that the Union:

- a. Reiterate existing credit card policies to staff and increase enforcement efforts to ensure that all credit card purchases are supported by sufficient and appropriate documentation and are promptly submitted to accounts payable for reconciliation.
- b. Ensure that all travel-related charges are reconciled to travel expense claim forms.

#### **Campus Response**

We concur. We will implement remedial actions, by the end of January 2011, to:

- a. Reiterate existing credit card policies to staff and increase enforcement efforts to ensure that all credit card purchases are supported by sufficient and appropriate documentation and are promptly submitted to accounts payable for reconciliation.
- b. Ensure that all travel-related charges are reconciled to travel expense claim forms.

## **PROPERTY AND EQUIPMENT**

The Union had not developed written policies and procedures to address completion of annual physical inventory counts, and adequate documentation was not maintained to show evidence of timely completion of the annual physical inventory.

We found that:

- ▶ Written policies and procedures had not been developed for current business practices concerning the completion of annual physical inventory counts.
- ▶ Adequate documentation was not maintained to show evidence of timely completion of the annual physical inventory, including reconciliation to the general ledger and review by management.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.7, *Property and Equipment*, states that the auxiliary should establish a written system that ensures physical inspection of property and equipment on a service life schedule, proper recording of property and equipment when received, and labeling of equipment. It further states that the auxiliary should reconcile physical inventories to the general ledger on a timely basis with review by management.

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

The Union associate director of administrative services stated that failure to develop written policies and procedures for annual physical inventory counts was due to oversight. She further stated that failure to maintain adequate documentation to show evidence of timely completion of the annual physical inventory was due to staffing constraints.

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

#### **Recommendation 41**

We recommend that Union:

- a. Develop written policies and procedures for current business practices concerning the completion of annual physical inventory counts.
- b. Ensure that the annual physical inventory is adequately documented, including reconciliation to the general ledger and review by management.

#### **Campus Response**

We concur. We will effectuate remedial actions, by the end of March 2011, to:

- a. Develop written policies and procedures for current business practices concerning the completion of annual physical inventory counts.
- b. Ensure that the annual physical inventory is adequately documented, including reconciliation to the general ledger and review by management.

## TRUSTS AND OTHER LIABILITIES

Funds held and administered by the Union on behalf of club sports were not supported by specific written agreements for each account.

Such agreements should address or consider the following areas:

- ▶ Purpose of the account.
- ▶ Source of funds.
- ▶ Reporting requirements.
- ▶ Time constraints.
- ▶ Instructions for closing the account.
- ▶ Disposition of unexpended balance.
- ▶ Administrative fees.
- ▶ Interest allocation.
- ▶ Applicable restrictions.

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 funds held and administered on behalf of others be properly supported by written agreements.

The Union associate director of administrative services stated that a Memorandum of Understanding (MOU) existed to formalize the agreement for the oversight of club sports but acknowledged that the MOU did not address or consider all necessary areas or address the specifics of each individual account.

The absence of written agreements increases the risk of misunderstandings and miscommunication regarding rights and responsibilities.

### **Recommendation 42**

We recommend that the Union establish written agreements for the administration and maintenance of funds held on behalf of club sports.

### **Campus Response**

We concur. We will establish written agreements for the administration and maintenance of funds held on behalf of club sports.

Expected completion date: By the end of January 2011

## **INFORMATION TECHNOLOGY**

### **DATA SECURITY**

Protected and/or sensitive data was not encrypted when stored in the Union accounting, payroll, and human resources systems.

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

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

The Union IT manager stated that the accounting, payroll, and human resources systems were off-the-shelf applications, and as such, the Union was limited in its ability to require the software vendors to make needed changes. He further stated that the Union had been evaluating without final approval some recent advances to both database systems and applications that allow for encryption.

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

#### **Recommendation 43**

We recommend that the Union apply encryption controls to all Union systems, computers, databases, and file servers that house protected and/or sensitive data.

#### **Campus Response**

We concur. We will apply encryption controls to all Union systems, computers, databases, and file servers that house protected and/or sensitive data.

Expected completion date: By the end of February 2011

### **USER ACCESS REVIEW**

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

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

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

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

The Union IT manager stated that he was unaware of the requirement to perform periodic, documented management reviews of user access privileges within Union systems. He further stated that user access was reviewed upon employee separation or job responsibility changes, but such reviews were not documented.

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

#### **Recommendation 44**

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

#### **Campus Response**

We concur. We will implement procedures to conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually.

Expected completion date: By the end of February 2011

#### **DATA CONFIDENTIALITY FORMS**

Union personnel with access to critical systems or protected data were not required to complete data confidentiality 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 that employees complete a data confidentiality form prior to being granted access to critical systems or protected data.

The Union IT manager stated that the Union had not required the completion of data confidentiality forms because it was unaware of this requirement. He added that employees agree to a basic confidentiality clause at time of hire, although this was not explicitly documented.

Failure to obtain data confidentiality forms from employees with access to critical systems or protected data increases the risk of inappropriate disclosure of data and auxiliary exposure to liability for any such disclosures.

#### **Recommendation 45**

We recommend that the Union establish a policy requiring data confidentiality forms from all employees prior to granting them access to critical systems and protected data, and obtain completed forms from personnel who currently have access to such systems and data.

#### **Campus Response**

We concur. We will establish a policy requiring data confidentiality forms from all employees prior to granting them access to critical systems and protected data, and obtain completed forms from personnel who currently have access to such systems and data.

Expected completion date: By the end of January 2011

### **VENDOR SERVICE AGREEMENTS**

Certain business arrangements between the Union and third-party systems vendors were not supported by complete and/or written agreements.

We found that:

- ▶ The business arrangement with a third-party service provider for payroll services was not supported by a written agreement. The payroll system, which contains protected employee data, was hosted off-site by the service provider. The lack of a service agreement for this off-site hosting service also resulted in information security and confidentiality terms not being adequately addressed.
- ▶ The service agreement with a third-party consultant that granted privileged system access to the accounting system, which contains protected data, lacked appropriate terms for information security and data confidentiality.

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.

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

The Union associate director of administrative services stated that the third-party payroll services provider had been used for many years and had provided sales orders, instead of service agreements, and they did not include specific security terms. She added that the Union was unaware of the requirement to include information security and data confidentiality terms within the service agreement with the third-party consultant that granted privileged system access to the accounting system.

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 auxiliary and CSU to potential liability.

#### **Recommendation 46**

We recommend that the Union:

- a. Establish a written agreement with the third-party payroll services provider and amend the consulting services agreement with appropriate provisions for information security and data confidentiality.
- b. Consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities (the most recent revision dated July 24, 2006, also includes a Section 42 for the confidentiality of data) for all vendor service agreements relating to access to protected records or data, or update its own standard agreement to include such references.

#### **Campus Response**

We concur. We will implement management procedures to effectuate compliance actions, by the end of February 2011, to:

- a. Establish a written agreement with the third-party payroll services provider and amend the consulting services agreement with appropriate provisions for information security and data confidentiality.
- b. Consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities (the most recent revision dated July 24, 2006, also includes a Section 42 for the confidentiality of data) for all vendor service agreements relating to access to protected records or data, or update our own standard agreement to include such references.

## **ENVIRONMENTAL CONTROLS**

The Union's server rooms located in the Student Union and Event Center lacked smoke detection devices.

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 fire detection devices be maintained within the premises of server rooms.

The Union IT manager stated that while smoke detectors were in close proximity to the server rooms, no smoke detectors were installed inside of these rooms. He added that this oversight was due to changes to the building infrastructure.

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

### **Recommendation 47**

We recommend that the Union install a smoke detection system in both server rooms.

### **Campus Response**

We concur. We will install a smoke detection system in both server rooms.

Expected completion date: By the end of January 2011

---

## **APPENDIX A: PERSONNEL CONTACTED**

### **Name**

### **Title**

#### **CAMPUS**

Don W. Kassing	Interim President
Jon Whitmore	President (at the time of review)
Rose Lee	Vice President, Administration and Finance
William McGuire	Vice President, Information Technology and Chief Information Officer
Ninh Pham-Hi	Director, Internal Control
Dorothy Poole	Assistant Vice President, Administration and Finance
Jaime Sanchez	Senior Director, Network Services and Information Security Officer

#### **SAN JOSÉ STATE UNIVERSITY RESEARCH FOUNDATION**

Cheree Aguilar	Human Resources Director
Adele Ajimura	Accounts Payable Supervisor
Sara Aujla	Special Assistant to the Chief Operating Officer
Jerri Carmo	Deputy Chief Operating Officer
Matt Cheung	Information Technology Manager
Jeanne Dittman	Associate Director, Sponsored Programs
Lan Duong	Associate Director, Post Award
Jeff Gordon	Director, Business and Community Partnerships
Paul Harris	Director, Finance and Accounting
Ranjit Kaur	Human Resources Coordinator
Kam Lam	Controller
Norma Rossiter	Associate Director, Business Services
Mary Sidney	Chief Operating Officer
Hoang Tran	Accountant III
John Troyan	Assistant Controller
Mila Valdez	Senior Cashier
Daisy Wan	Senior Accountant

#### **THE TOWER FOUNDATION**

Nancy Bussani	Chief Operating Officer and Associate Vice President, Advancement Operations
Leslie Rohn	Controller

#### **SPARTAN SHOPS, INC.**

Ann Bui	Director of Accounting/Administration and Finance
Ryan Chiangi	Interim Textbook Manager
Scott Cofer	Warehouse Manager
Jennifer Goodale	Assistant Director of Residential Operations
Jason Hood	Manager of Retail Operations
Rose Hunter	Catering Manager
Jay Marshall	Catering Chef
Jerry Mimnaugh	Executive Director

### **SPARTAN SHOPS, INC. (CONT.)**

Brian Mitchler	Manager of Residential Dining
Bill Mowson	Cashier's Office Manager
Steven Olesen	Assistant Director of Procurement
Jeff Pauley	Director of Dining Services
Ryan Ptucha	Manager of Retail Operations
Beth Pugliese	Senior Director of Commercial Services
Ivy Romero	Accounting Manager
Jennifer Skebba	Manager of Retail Services
Lisa Thomas	Director of Human Resources
Trisha Vo	Payroll Administrator
Mike Yin	Director of Information Technology and Services

### **ASSOCIATED STUDENTS SAN JOSÉ STATE UNIVERSITY**

Shawn Chan	Finance and Accounting Manager
Paul Lee	Print Shop Manager
Helen Nguyen	Accountant
Vivian Nguyen	Supervisor/Cashier
Analisa Perez	Administrative Assistant, Child Development Center
Jennifer Pourshahidi	Human Resources Coordinator
Fran Roth	Information Technology Manager
Randy Saffold	Campus Recreation Manager
Jason Stovall	Director, Child Development Center
Nancy Tepperman	Administrative Assistant, Child Development Center
Trinh Thai	Senior Accountant
Kevin Tran	Operations Coordinator, Computer Services Center
Cheryl Vargas	Executive Director

### **THE STUDENT UNION OF SAN JOSÉ STATE UNIVERSITY**

Gloria Acoba	Box Office Manager
Cathy Busalacchi	Executive Director
Jerry Darrell	Information Technology Manager
Sharon Deaver	Bowling Center Manager
Connie Guan	Accounts Receivable Accounting Technician
Kim Hagens	Accounting Manager
Rebecca Harper	Aquatic Center Coordinator
Kristin Kelly	Associate Director, Administrative Services
Mary Lewis	Human Resources Manager
Leanne LoBue	Scheduling Supervisor
Caryn Murray	Recreation Facilities Manager
My Phuong Tran	Accounts Payable Accounting Technician

## **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.



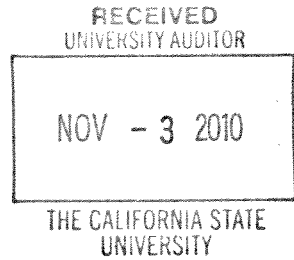
**San José State**  
UNIVERSITY

**Office of the Vice President  
for Administration and  
Finance**

One Washington Square  
San José, CA 95192-0006  
Voice: 408-924-1500  
Fax: 408-924-1515  
<http://www.sjsu.edu>



November 3, 2010



Mr. Larry Mandel  
University Auditor  
The California State University  
401 Golden Shore, 4<sup>th</sup> Floor  
Long Beach, CA 90802

**Campus Response to Auxiliary Audit (10-02) at  
San José State University.**

Enclosed is San José State University's response to the Auxiliary Audit (10-02). The campus is committed to addressing the issues identified in this audit report.

Please let me know if I can provide you with additional information.

A handwritten signature in cursive that reads "Rose L. Lee".

Rose L. Lee  
Vice President for Administration and Finance

Enclosure

cc: Don W. Kassing, Interim President  
Ninh Pham-Hi, Director, Internal Control

**The California State University:**

Chancellor's Office, Bakersfield, Channel Islands, Chico, Dominguez Hills, East Bay, Fresno, Fullerton, Humboldt, Long Beach, Los Angeles, Maritime Academy, Monterey Bay, Northridge, Pomona, Sacramento, San Bernardino, San Diego, San Francisco, San José, San Louis Obispo, San Marcos, Sonoma, Stanislaus

**AUXILIARY ORGANIZATIONS  
SAN JOSÉ STATE UNIVERSITY**

**Audit Report 10-02**

**CAMPUS**

**INFORMATION TECHNOLOGY**

**Recommendation 1**

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

**Campus Response**

We concur. We will develop and implement an action plan for providing information security awareness training to all auxiliary employees with access to critical systems or protected data. By end of January 2011.

## SAN JOSÉ STATE UNIVERSITY RESEARCH FOUNDATION

### PROPERTY AND EQUIPMENT

#### Recommendation 2

We recommend that the Foundation document its management review of the annual physical inventory.

#### Campus Response

We concur. We will document the management review of the annual physical inventory. By end of February 2011.

### TRUSTS AND OTHER LIABILITIES

#### Recommendation 3

We recommend that the Foundation:

- a. Complete a review of all campus programs and projects accounts and determine, within 60 days, which accounts contain state/campus operating funds.
- b. Certify that none of the following specific and similar monies reside in Foundation accounts:
  - Contracts and grants awarded to the university.
  - Foundation net operating surplus designated for use by the campus.
  - Fees for continuing education courses provided by the university.
  - Fees for university events, workshops, conferences, institutes, special projects, and programs.
  - Athletics funds/fees/revenues other than gifts/donations.
  - Investment income from state funds/fees/revenues.
  - Reimbursements for services and products provided to auxiliary enterprises and organizations paid from General Fund and/or CSU operating fund monies.
  - Rental fees for university facilities, except those facilities that have been leased to the auxiliary by the campus.
  - Student fees and other general fees pursuant to the CSU student fee policy.
  - Monies held by the Foundation via contract with the campus.

- c. Submit to the Office of the University Auditor, within 60 days, a list of those accounts that have been deemed appropriate to remain in the custody of the Foundation and comprehensive documentation to support the sources of funds for those trust accounts.
- d. Move those state funds identified in “a” above to campus accounts within six months.
- e. Ensure that trust account agreements are prepared for all campus programs and projects accounts to clearly document the purpose of the accounts and required approvals.

#### **Campus Response**

We concur. We will complete a review of all campus programs and projects and provide certification as required above and by Executive Order 1052, by the deadline given in Executive Order 1052.

## **INFORMATION TECHNOLOGY**

### **PASSWORD AND DATA SECURITY**

#### **Recommendation 4**

We recommend that the Foundation:

- a. Set effective password and login security parameters for the payroll system in accordance with leading information security industry guidelines and perform an assessment of password security parameters for all other Foundation systems.
- b. Apply encryption controls to the accounting and payroll systems and all other Foundation systems, computers, databases, and file servers that house protected and/or sensitive data.

#### **Campus Response**

We concur. We will complete remedial action by end of February 2011, to:

- a. Set effective password and login security parameters for the payroll system in accordance with leading information security industry guidelines and perform an assessment of password security parameters for all other Foundation systems.
- b. Apply encryption controls to the accounting and payroll systems and all other Foundation systems, computers, databases, and file servers that house protected and/or sensitive data.

### **EQUIPMENT TRACKING AND SECURITY**

#### **Recommendation 5**

We recommend that the Foundation ensure the security of and maintain an inventory of all computing equipment purchased by the Foundation, including those purchased via grant funding.

**Campus Response**

We concur. We will ensure the security of and maintain an inventory of all computing equipment purchased by the Foundation, including those purchased via grant funding. By end of March 2011.

**NETWORK SECURITY****Recommendation 6**

We recommend that the Foundation perform an assessment and evaluate the feasibility of implementing a DMZ to separate and protect internal Foundation resources from Internet-accessible devices.

**Campus Response**

We concur. We will perform an assessment and evaluate the feasibility of implementing a DMZ to separate and protect internal Foundation resources from Internet-accessible devices. By end of March 2011.

**REMOTE ACCESS SECURITY****Recommendation 7**

We recommend that the Foundation replace Telnet remote access with a more secure remote access protocol (such as Secure Shell) or enforce internal firewall restrictions on Telnet such that it could only be accessed once a virtual private network connection has been established.

**Campus Response**

We concur. We will either replace Telnet remote access with a more secure remote access protocol (such as Secure Shell) or enforce internal firewall restrictions on Telnet such that it could only be accessed once a virtual private network connection has been established. By end of February 2011.

**USER ACCESS REVIEW****Recommendation 8**

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

**Campus Response**

We concur. We will implement procedure to conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually. By end of March 2011.

## **SYSTEM BACKUPS**

### **Recommendation 9**

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

### **Campus Response**

We concur. We will encrypt system backups of protected data and ensure that the off-site transfer and storage of backups is secure. By end of February 2011.

## THE TOWER FOUNDATION

### OPERATING AND ADMINISTRATIVE AGREEMENTS

#### Recommendation 10

We recommend that the TF:

- a. Amend the cited agreement with an appropriate indemnification and right-to-audit clause.
- b. Ensure that all future agreements with third parties include an appropriate indemnification provision and a right-to-audit clause.

#### Campus Response

We concur. We implemented the compliance action in May 2010, to:

- a. Amend the cited agreement with an appropriate indemnification and right-to-audit clause.
- b. Ensure that all future agreements with third parties include an appropriate indemnification provision and a right-to-audit clause.

### CORPORATE GOVERNANCE

#### Recommendation 11

We recommend that the TF promptly file the cited amendments with the Financing and Treasury department at the Office of the Chancellor and ensure that all future changes/amendments to Bylaws are filed within 30 calendar days.

#### Campus Response

We concur. We have filed the cited amendments with the Financing and Treasury department at the Office of the Chancellor in May 2010 and have issued management reminder to ensure that all future changes/amendments to Bylaws are filed within 30 calendar days.

### PURCHASING AND ACCOUNTS PAYABLE

#### DISBURSEMENTS

#### Recommendation 12

We recommend that the TF:

- a. Obtain two signatures on all checks over \$5,000, as required by TF policy.

- b. Obtain signed release forms/waivers from each student traveling by air on campus-program-sponsored trips.
- c. Reiterate to staff existing procurement policy regarding competitive bidding.

**Campus Response**

We concur. We will implement procedure to effectuate remedial actions, by end of February 2011, to:

- a. Obtain two signatures on all checks over \$5,000, as required by TF policy.
- b. Obtain signed release forms/waivers from each student traveling by air on campus-program-sponsored trips.
- c. Reiterate to staff existing procurement policy regarding competitive bidding.

**TRAVEL AUTHORIZATION**

**Recommendation 13**

We recommend that the TF revise its travel policy to require completion of travel request forms prior to travel and ensure that the travel requests are properly reviewed and approved.

**Campus Response**

We concur. We will revise the travel policy to require completion of travel request forms prior to travel and ensure that the travel requests are properly reviewed and approved. By end of January 2011.

**ENDOWMENT ADMINISTRATION**

**Recommendation 14**

We recommend that the TF update its endowment agreement to specifically address the TF's administrative fees and ensure that all donors are notified of the administrative fees.

**Campus Response**

We concur. We have updated the endowment agreement template to specifically address the TF's administrative fees in October 2010 and have issued management reminder to ensure that all donors are notified of the administrative fees.

## **INFORMATION TECHNOLOGY**

### **PASSWORD SECURITY**

#### **Recommendation 15**

We recommend that the TF set effective password and login security parameters for the accounting and donor systems in accordance with leading information security industry guidelines and perform an assessment of password security parameters for all other TF systems.

#### **Campus Response**

We concur. We will set effective password and login security parameters for the accounting and donor systems in accordance with leading information security industry guidelines and perform an assessment of password security parameters for all other TF systems. By end of January 2011.

### **USER ACCESS REVIEW**

#### **Recommendation 16**

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

#### **Campus Response**

We concur. We will implement procedure to conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually. By end of February 2011.

### **DISASTER RECOVERY PLAN**

#### **Recommendation 17**

We recommend that the campus and TF collaborate to complete a comprehensive IT DRP that includes all critical systems.

#### **Campus Response**

We concur. We will design a comprehensive IT DRP that includes all critical systems. By end of March 2011.

**SPARTAN SHOPS, INC.****OPERATIONAL COMPLIANCE****POLICIES AND PROCEDURES****Recommendation 18**

We recommend that Shops develop written policies and procedures to address the operation and administration of the Gold Points program, including recording and administration of Gold Points subsequent to the deposit of funds by students and the administration of outstanding/idle Gold Points for students no longer enrolled at the university.

**Campus Response**

We concur. We will develop written policies and procedures to address the operation and administration of the Gold Points program, including recording and administration of Gold Points subsequent to the deposit of funds by students and the administration of outstanding/idle Gold Points for students no longer enrolled at the university. By end of February 2011.

**RISK MANAGEMENT****Recommendation 19**

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

**Campus Response**

We concur. We will develop and adopt a written risk management policy, including procedures to actively identify, analyze, quantify, and manage risk. By end of March 2011.

**INVENTORY MANAGEMENT****Recommendation 20**

We recommend that Shops:

- a. Review and revise its inventory management controls to ensure the accuracy of merchandise perpetual inventory records.
- b. Perform documented management reviews of merchandise price changes on a routine basis, such as monthly.

**Campus Response**

We concur. We will implement management procedures to effectuate compliance action, by end of February 2011, to:

- a. Review and revise the inventory management controls to ensure the accuracy of merchandise perpetual inventory records.
- b. Perform documented management reviews of merchandise price changes on a routine basis, such as monthly.

## **CASH RECEIPTS AND HANDLING**

### **Recommendation 21**

We recommend that Shops:

- a. Update the Shops' cash shortage policy/procedure to require documentation of investigations and ensure proper documentation of cash shortage and/or overage investigations.
- b. Record checks to the check receipt log in a timely manner.
- c. Perform timely bank reconciliations.

### **Campus Response**

We concur. We will implement management procedures to effectuate compliance action, by end of January 2011, to:

- a. Update the Shops' cash shortage policy/procedure to require documentation of investigations and ensure proper documentation of cash shortage and/or overage investigations.
- b. Record checks to the check receipt log in a timely manner.
- c. Perform timely bank reconciliations.

## **PETTY CASH AND CHANGE FUNDS**

### **Recommendation 22**

We recommend that Shops:

- a. Develop and implement written policies for periodic, independent cash counts of petty cash.
- b. Perform and document periodic, independent cash counts of all petty cash.
- c. Perform and document independent cash counts of cash vault funds as required by Vault Policies.

**Campus Response**

We concur. We will implement management procedures to effectuate compliance action, by end of January 2011, to:

- a. Develop and implement written policies for periodic, independent cash counts of petty cash.
- b. Perform and document periodic, independent cash counts of all petty cash.
- c. Perform and document independent cash counts of cash vault funds as required by Vault Policies.

**FEEES, REVENUES, AND RECEIVABLES****Recommendation 23**

We recommend that Shops complete its evaluation of errors and dysfunctions identified within the new ERP system, including the erroneous accounting of POS cash sales transactions as accounts receivable, and take action for prompt resolution.

**Campus Response**

We concur. We will complete the evaluation of errors and dysfunctions identified within the new ERP system, including the erroneous accounting of POS cash sales transactions as accounts receivable, and take action for prompt resolution. By end of February 2011.

**PERSONNEL AND PAYROLL****Recommendation 24**

We recommend that Shops reiterate to all employees the vacation time off request policy requirements to ensure that all requests are documented and approved by management.

**Campus Response**

We concur. We will reiterate to all employees the vacation time off request policy requirements to ensure that all requests are documented and approved by management. By end of January 2011.

**PROPERTY AND EQUIPMENT****Recommendation 25**

We recommend that Shops perform a periodic, independent physical inventory of its property and equipment, including reconciliation to the general ledger, with review by management.

**Campus Response**

We concur. We will implement management procedure to perform a periodic, independent physical inventory of property and equipment, including reconciliation to the general ledger, with review by management. By end of February 2011.

## INFORMATION TECHNOLOGY

### DATA SECURITY

#### Recommendation 26

We recommend that Shops apply encryption controls to all Shops systems, computers, databases, and file servers that house protected and/or sensitive data.

#### Campus Response

We concur. We will apply encryption controls to all Shops systems, computers, databases, and file servers that house protected and/or sensitive data. By end of February 2011.

### USER ACCESS REVIEW

#### Recommendation 27

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

#### Campus Response

We concur. We will conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually. By end of February 2011.

### DISASTER RECOVERY PLAN

#### Recommendation 28

We recommend that Shops complete a comprehensive IT DRP that is inclusive of all critical systems.

#### Campus Response

We concur. We will design a comprehensive IT DRP that is inclusive of all critical systems. By end of March 2011

### SYSTEM BACKUPS

#### Recommendation 29

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

#### Campus Response

We concur. We will encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure. By end of February 2011.

## **ASSOCIATED STUDENTS SAN JOSÉ STATE UNIVERSITY**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS**

#### **Recommendation 30**

We recommend that AS promptly renew its operating agreement with the CSU Trustees and implement a process to ensure that future agreements are renewed in a timely fashion.

#### **Campus Response**

We concur. We will renew the operating agreement with the CSU Trustees and implement a process to ensure that future agreements are renewed in a timely fashion. By end of January 2011.

### **OPERATIONAL COMPLIANCE**

#### **Recommendation 31**

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. We will develop and adopt a written and consolidated risk management policy, including procedures to actively identify, analyze, quantify, and manage risk. By end of February 2011.

### **SEGREGATION OF DUTIES**

#### **Recommendation 32**

We recommend that AS revoke administrative rights access to the payroll system for employees with payroll processing duties.

#### **Campus Response**

We concur. We will implement procedure to revoke administrative rights access to the payroll system for employees with payroll processing duties. By end of January 2011.

### **CASH RECEIPTS AND HANDLING**

#### **Recommendation 33**

We recommend that AS:

- a. Localize accountability over cash receipts when multiple cashiers operate the same register.

- b. Update daily close-out procedures to include an independent count of each cashier's drawer by a supervisor or other staff member.
- c. Update daily opening procedures to include a count of the opening banks for each cash register to verify the beginning amount of cash.
- d. Place the safe in a secure location, keep the safe locked during business hours, and restrict access to the safe to only those employees with a business need for such access.

### **Campus Response**

We concur. We will implement procedures to effectuate compliance actions, by end of January 2011, to:

- a. Localize accountability over cash receipts when multiple cashiers operate the same register.
- b. Update daily close-out procedures to include an independent count of each cashier's drawer by a supervisor or other staff member.
- c. Update daily opening procedures to include a count of the opening banks for each cash register to verify the beginning amount of cash.
- d. Place the safe in a secure location, keep the safe locked during business hours, and restrict access to the safe to only those employees with a business need for such access.

## **INFORMATION TECHNOLOGY**

### **DATA SECURITY**

#### **Recommendation 34**

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

#### **Campus Response**

We concur. We will design encryption controls to all AS systems, computers, databases, and file servers that house protected and/or sensitive data. By end of February 2011.

### **USER ACCESS REVIEW**

#### **Recommendation 35**

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

**Campus Response**

We concur. We will implement procedure to conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually. By end of February 2011.

**SYSTEM BACKUPS**

**Recommendation 36**

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

**Campus Response**

We concur. We will encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure. By end of February 2011.

**THE STUDENT UNION OF SAN JOSÉ STATE UNIVERSITY**

**FISCAL COMPLIANCE**

**Recommendation 37**

We recommend that the Union update its reserve policy to reflect current practice.

**Campus Response**

We concur. We will update the reserve policy to reflect current practice. By end of January 2011.

**CASH RECEIPTS AND HANDLING**

**Recommendation 38**

We recommend that the Union:

- a. Localize accountability over cash receipts when multiple cashiers operate the same register at the Event Center box office.
- b. Designate back-up personnel for verification and deposit of cash receipts at the Event Center box office.
- c. Establish written policy and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery.

**Campus Response**

We concur. We will implement procedures to effectuate compliance actions, by end of February 2011, to:

- a. Localize accountability over cash receipts when multiple cashiers operate the same register at the Event Center box office.
- b. Designate back-up personnel for verification and deposit of cash receipts at the Event Center box office.
- c. Establish written policy and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery.

**INVESTMENTS**

**Recommendation 39**

We recommend that the Union promptly update the signature authorization for its investment accounts to reflect the change in the chair of the board of directors.

**Campus Response**

We concur. We will update the signature authorization for its investment accounts to reflect the change in the chair of the board of directors. By end of January 2011.

**PURCHASING AND ACCOUNTS PAYABLE****Recommendation 40**

We recommend that the Union:

- a. Reiterate existing credit card policies to staff and increase enforcement efforts to ensure that all credit card purchases are supported by sufficient and appropriate documentation and are promptly submitted to accounts payable for reconciliation.
- b. Ensure that all travel-related charges are reconciled to travel expense claim forms.

**Campus Response**

We concur. We will implement remedial actions, by end of January 2011, to:

- a. Reiterate existing credit card policies to staff and increase enforcement efforts to ensure that all credit card purchases are supported by sufficient and appropriate documentation and are promptly submitted to accounts payable for reconciliation.
- b. Ensure that all travel-related charges are reconciled to travel expense claim forms.

**PROPERTY AND EQUIPMENT****Recommendation 41**

We recommend that Union:

- a. Develop written policies and procedures for current business practices concerning the completion of annual physical inventory counts.
- b. Ensure that the annual physical inventory is adequately documented, including reconciliation to the general ledger and review by management.

**Campus Response**

We concur. We will effectuate remedial actions, by end of March 2011, to:

- a. Develop written policies and procedures for current business practices concerning the completion of annual physical inventory counts.
- b. Ensure that the annual physical inventory is adequately documented, including reconciliation to the general ledger and review by management.

## TRUSTS AND OTHER LIABILITIES

### Recommendation 42

We recommend that the Union establish written agreements for the administration and maintenance of funds held on behalf of club sports.

### Campus Response

We concur. We will establish written agreements for the administration and maintenance of funds held on behalf of club sports. By end of January 2011.

## INFORMATION TECHNOLOGY

### DATA SECURITY

#### Recommendation 43

We recommend that the Union apply encryption controls to all Union systems, computers, databases, and file servers that house protected and/or sensitive data.

#### Campus Response

We concur. We will apply encryption controls to all Union systems, computers, databases, and file servers that house protected and/or sensitive data. By end of February 2011.

### USER ACCESS REVIEW

#### Recommendation 44

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

#### Campus Response

We concur. We will implement procedure to conduct periodic, documented management reviews of user access for all critical systems and applications containing protected data, at least annually. By end of February 2011.

### DATA CONFIDENTIALITY FORMS

#### Recommendation 45

We recommend that the Union establish a policy requiring data confidentiality forms from all employees prior to granting them access to critical systems and protected data, and obtain completed forms from personnel who currently have access to such systems and data.

**Campus Response**

We concur. We will establish a policy requiring data confidentiality forms from all employees prior to granting them access to critical systems and protected data, and obtain completed forms from personnel who currently have access to such systems and data. By end of January 2011.

**VENDOR SERVICE AGREEMENTS****Recommendation 46**

We recommend that the Union:

- a. Establish a written agreement with the third-party payroll services provider and amend the consulting services agreement with appropriate provisions for information security and data confidentiality.
- b. Consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities (the most recent revision dated July 24, 2006, also includes a Section 42 for the confidentiality of data) for all vendor service agreements relating to access to protected records or data, or update its own standard agreement to include such references.

**Campus Response**

We concur. We will implement management procedures to effectuate compliance actions, by end of February 2011, to:

- a. Establish a written agreement with the third-party payroll services provider and amend the consulting services agreement with appropriate provisions for information security and data confidentiality.
- b. Consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities (the most recent revision dated July 24, 2006, also includes a Section 42 for the confidentiality of data) for all vendor service agreements relating to access to protected records or data, or update its own standard agreement to include such references.

**ENVIRONMENTAL CONTROLS****Recommendation 47**

We recommend that the Union install a smoke detection system in both server rooms.

**Campus Response**

We concur. We will install a smoke detection system in both server rooms. By end of January 2011.

THE CALIFORNIA STATE UNIVERSITY  
OFFICE OF THE CHANCELLOR

BAKERSFIELD

CHANNEL ISLANDS

November 24, 2010

CHICO

**MEMORANDUM**

DOMINGUEZ HILLS

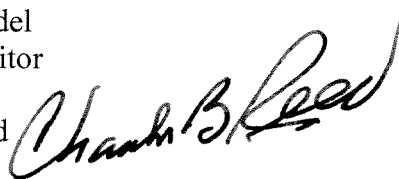
EAST BAY

TO: Mr. Larry Mandel  
University Auditor

FRESNO

FULLERTON

FROM: Charles B. Reed  
Chancellor



HUMBOLDT

SUBJECT: Draft Final Report 10-02 on *Auxiliary Organizations*,  
San José State University

LONG BEACH

LOS ANGELES

In response to your memorandum of November 24, 2010, I accept the response as submitted with the draft final report on *Auxiliary Organizations*, San José State University.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/amd

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS