AUXILIARY ORGANIZATIONS

CALIFORNIA STATE UNIVERSITY,
FULLERTON

Audit Report 09-13
July 29, 2009

Members, Committee on Audit

Melinda Guzman, Chair
Raymond W. Holdsworth, Vice Chair
Herbert L. Carter Carol R. Chandler
Kenneth Fong Margaret Fortune
George G. Gowgani William Hauck
Henry Mendoza

Staff

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

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
CONTENTS

CSU FULLERTON PHILANTHROPIC FOUNDATION
Fiscal Compliance ................................................................. 31
Operational Compliance ....................................................... 31
Fees, Revenues, and Receivables ........................................... 32
Endowment Administration .................................................... 33
Information Technology ........................................................ 34

ASSOCIATED STUDENTS CALIFORNIA STATE UNIVERSITY, FULLERTON, INC.
Fiscal Compliance ................................................................. 36
Cash Receipts and Handling .................................................... 37
Fees, Revenues, and Receivables ........................................... 38
Purchasing and Accounts Payable ........................................... 39
Information Technology ........................................................ 41
  Password Security .............................................................. 41
  Environmental Controls ....................................................... 42

CSU FULLERTON HOUSING AUTHORITY
Corporate Governance .......................................................... 44
Segregation of Duties ........................................................... 45
Purchasing and Accounts Payable .......................................... 45
APPENDICES

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

ABBREVIATIONS

AS  Associated Students California State University, Fullerton, Inc.
CFO  Chief Financial Officer
CIO  Chief Information Officer
Corporation  CSU Fullerton Auxiliary Services Corporation
CSU  California State University
CSUF  California State University, Fullerton
DMZ  Demilitarized Zone
EO  Executive Order
Foundation  CSU Fullerton Philanthropic Foundation
FTP  File Transfer Protocol
Housing Authority  CSU Fullerton Housing Authority
IFAS  Integrated Financial and Accounting System
IRS  Internal Revenue Service
MBS  Missouri Book System
MIS  Management Information Systems
OMB  Office of Management and Budget
PCI DSS  Payment Card Industry Data Security Standard
RFIN  Resolution of the Committee on Finance
SAQ  Self-Assessment Questionnaire
Teletelnet  Telecommunication Network
UBI  Unrelated Business Income
VPN  Virtual Private Network
EXECUTIVE SUMMARY

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

California State University, Fullerton (CSUF) 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 CSUF campus and its auxiliary organizations from February 2, 2009, through March 6, 2009, and made a study and evaluation of the system of internal compliance/internal control in effect as of March 6, 2009. This report represents our triennial review.

Our study and evaluation at CSU Fullerton Auxiliary Services Corporation revealed certain conditions that, in our opinion, could result in errors and irregularities if not corrected. Specifically, the auxiliary did not maintain adequate control over information technology. One of the 14 findings was also a repeat from the prior auxiliary organizations audit. These conditions, along with other weaknesses, are described in the executive summary and in the body of the report. In our opinion, except for the effect of the weaknesses described above, accounting and administrative control in effect as of March 6, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at the CSU Fullerton Philanthropic Foundation did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. However, we did identify other reportable weaknesses that are described in the executive summary and in the body of the report. In our opinion, the accounting and
administrative control in effect as of March 6, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at Associated Students California State University, Fullerton, Inc. did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. However, we did identify two repeat findings from the prior auxiliary organizations audit and other reportable weaknesses that are described in the executive summary and in the body of the report. In our opinion, the accounting and administrative control in effect as of March 6, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at the CSU Fullerton Housing Authority did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. However, we did identify other reportable weaknesses that are described in the executive summary and in the body of the report. In our opinion, the accounting and administrative control in effect as of March 6, 2009, taken as a whole, was sufficient to meet the objectives stated above.

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

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

**CAMPUS**

**FISCAL COMPLIANCE [11]**

Annual auxiliary cost allocation analyses for the reimbursement of costs incurred by the university were neither completed timely nor formally approved by the campus chief financial officer or his designee.

**INFORMATION TECHNOLOGY [12]**

The campus did not ensure that the auxiliaries had fully addressed Payment Card Industry (PCI) Data Security Standard requirements. In addition, the CSU Fullerton Auxiliary Services Corporation, CSU Fullerton Philanthropic Foundation and Associated Students California State University, Fullerton, Inc., did not perform periodic, documented management reviews of user access privileges within all systems and applications containing protected data, or require that personnel with access to protected data complete information security awareness training.
EXECUTIVE SUMMARY

CSU FULLERTON AUXILIARY SERVICES CORPORATION

OPERATING AND ADMINISTRATIVE AGREEMENTS [16]

Certain business arrangements between the CSU Fullerton Auxiliary Services Corporation (Corporation) and third parties were not supported by complete and/or current written agreements.

CORPORATE GOVERNANCE [17]

The Corporation did not have the required number of community directors on its governing board for fiscal years 2006/07, 2007/08 and 2008/09.

OPERATIONAL COMPLIANCE [18]

The Corporation did not track the transfer of inventory from the bookstore centralized receiving dock to satellite locations.

PROGRAM COMPLIANCE [18]

The Corporation had neither established nor implemented a process to report to the campus financial aid office stipends paid to student interns working for the Titan Daily newspaper.

CASH RECEIPTS AND HANDLING [19]

The Corporation had not developed written policies and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery.

TRUSTS AND OTHER LIABILITIES [20]

Certain campus program revenues were inappropriately deposited to, and held in custody by, the Corporation.

AUXILIARY PROGRAMS [21]

Cost share and effort certification reports were not always prepared at the Corporation.

INFORMATION TECHNOLOGY [22]

Password controls and security parameters were not always adequate for Corporation systems. This is a repeat finding from the prior auxiliary organizations audit. The Corporation had not adequately secured certain systems and files containing critical and/or sensitive data, nor performed an assessment and inventory of protected data residing on an administrative file server. Further, Corporation personnel with access to critical systems and protected data were not required to complete data confidentiality forms. In addition, backups for Corporation systems were not adequately controlled, remote access to Corporation
servers was not always secure, and the Corporation had not completed a written information technology disaster recovery plan. Also, the Corporation data center had a water-sprinkler system which could be detrimental to the electrical equipment housed in the data center, and several of the servers were not elevated above the floor in the event of flooding.

**CSU FULLERTON PHILANTHROPIC FOUNDATION**

**FISCAL COMPLIANCE [31]**

The CSU Fullerton Philanthropic Foundation (Foundation) had not developed a written reserve policy.

**OPERATIONAL COMPLIANCE [31]**

The Foundation had not developed a written risk management policy.

**FEES, REVENUES, AND RECEIVABLES [32]**

Storage of donation forms and documentation containing credit card information from donors was not in compliance with PCI standards at the Foundation.

**ENDOWMENT ADMINISTRATION [33]**

Certain Foundation endowment files lacked executed endowment agreements, and some endowment agreements did not delineate management fees and/or the annual spending policy.

**INFORMATION TECHNOLOGY [34]**

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

**ASSOCIATED STUDENTS CALIFORNIA STATE UNIVERSITY, FULLERTON, INC.**

**FISCAL COMPLIANCE [36]**

Unrelated business income for the Titan Bowl and Billiards was not properly accounted for/reported by Associated Students California State University, Fullerton, Inc.

**CASH RECEIPTS AND HANDLING [37]**

The transfer of AS cash receipts was not adequately documented and safeguarded.
EXECUTIVE SUMMARY

FEES, REVENUES, AND RECEIVABLES [38]

AS collection activity and follow-up on past-due agency and third-party accounts receivables were not adequate to ensure collection. In addition, policies and procedures had not been documented for the monitoring of accounts receivable, collection of delinquent agency accounts and third-party receivables, and bad debt write-offs.

PURCHASING AND ACCOUNTS PAYABLE [39]

Certain AS cash disbursements were neither supported by sufficient and appropriate documentation nor appropriately authorized. The processing exceptions were all repeat findings from the prior auxiliary organizations audit.

INFORMATION TECHNOLOGY [41]

Password security parameters were not always adequate for AS systems, and system administrators were unable to review and change security parameters for several critical systems. In addition, the AS server room lacked fire or smoke detection devices, although a fire extinguisher was located within the room.

CSU FULLERTON HOUSING AUTHORITY

CORPORATE GOVERNANCE [44]

The CSU Fullerton Housing Authority (Housing Authority) had not filed amended Articles of Incorporation with the chancellor’s office in a timely manner.

SEGREGATION OF DUTIES [45]

Certain duties and responsibilities related to cash receipts processing were not adequately segregated at the Housing Authority.

PURCHASING AND ACCOUNTS PAYABLE [45]

Housing Authority oversight of purchasing activities performed by a third-party property management firm for University Gables and University Heights, as well as the reimbursement of activities performed by a real estate agent, were not adequate.
INTRODUCTION

BACKGROUND

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

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

- Institute a standard systemwide accounting and reporting system for businesslike management of the operation of such auxiliary organizations.

- Implement financial standards that will assure the fiscal viability of such various auxiliary organizations. Such standards shall include proper provision for professional management, adequate working capital, adequate reserve funds for current operations and capital replacements, and adequate provisions for new business requirements.

- Institute procedures to assure that transactions of the auxiliary organizations are within the educational mission of the state colleges.

- Develop policies for the appropriation of funds derived from indirect cost payments.

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

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

The CSU Fullerton Auxiliary Services Corporation (Corporation) was established in 1959 as a non-profit public benefit corporation for the purpose of promoting and assisting CSU Fullerton (CSUF) in fulfilling its mission. The Corporation is responsible for commercial operations, including bookstore and dining services, post-award administration of sponsored programs; and fiscal administration of numerous campus programs, such as centers and institutes. Further, the Corporation administers the College Park building to provide additional offices and classrooms for the campus.
INTRODUCTION

The CSU Fullerton Philanthropic Foundation (Foundation) was established in 1998 as a tax-exempt, charitable and educational organization. The Foundation supports CSUF through fundraising, acceptance of donor gifts, and management of endowments. The Foundation also works closely with and is supported in its fundraising efforts by University Advancement. The Foundation works with alumni and the community to secure gifts and to generate funds that allow CSUF to continue its educational mission.

Associated Students California State University, Fullerton, Inc. (AS) is a non-profit auxiliary corporation incorporated in September 1975 and formed for the specific and primary purpose of operating a charitable and educational organization. The AS is charged with operating the student body government, the Children’s Center, the Titan Student Union, and the Student Recreation Center, as well as providing the campus community with social, cultural, educational, and entertainment opportunities. AS is governed by the Student Board of Directors and employs an executive director and numerous management and staff personnel to manage daily operations.

The CSU Fullerton Housing Authority (Housing Authority) is a non-profit public benefit corporation responsible for the development, provision, and maintenance of affordable housing and other related facilities and activities for the use and convenience of faculty and staff of the university, in order to foster an academic community and environment on or near the campus, and to attract and retain the highest quality faculty and staff at the university. The Housing Authority is a single-purpose auxiliary with no dedicated employees, property management services have been outsourced to Encore Property Management, and all administrative and accounting services are provided by the Corporation. The Housing Authority oversees the rental program and the construction, financing, sales, and re-sales of the for-sale program, plus community/property management. The Housing Authority is independently managed and governance is provided by a nine member board of directors comprised of campus management and staff, faculty, non-campus personnel, and students.

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.
INTRODUCTION

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 2006/07 and 2007/08 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, 2008, to March 6, 2009. Our primary focus was on internal compliance/internal control.

Specifically, we reviewed and tested:

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

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

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

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

**CSU Fullerton Auxiliary Services Corporation**
- Operating and Administrative Agreements
- Facilities Agreements
- Corporate Governance
- Fiscal Compliance
- Operational Compliance
- Program Compliance
INTRODUCTION

CSU Fullerton Auxiliary Services Corporation (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

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

Associated Students California State University, Fullerton, 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
INTRODUCTION

Associated Students California State University, Fullerton, Inc. (cont.)
› Trusts and Other Liabilities
› Auxiliary Programs
› Information Technology

CSU Fullerton Housing Authority
› Operating and Administrative Agreements
› Facilities Agreements
› Corporate Governance
› Fiscal Compliance
› Operational Compliance
› Program Compliance
› Campus Oversight and Control
› Segregation of Duties
› Cash Receipts and Handling
› Investments
› Fees, Revenues, and Receivables
› Purchasing and Accounts Payable

Campus
› Campus Oversight and Control

We have not performed any auditing procedures beyond March 6, 2009. Accordingly, our comments are based on our knowledge as of that date. Since the purpose of our comments is to suggest areas for improvement, comments on favorable matters are not addressed.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

CAMPUS

FISCAL COMPLIANCE

Annual auxiliary cost allocation analyses for the reimbursement of costs incurred by the university were neither completed timely nor formally approved by the campus chief financial officer (CFO) or his designee.

We found that:

› The CSU Fullerton Auxiliary Services Corporation (Corporation) cost allocation analysis for fiscal year 2007/08 had not been signed and dated evidencing campus CFO approval of post-year calculations. This is a repeat finding from the November 2007 Contracts and Grants audit.

› The CSU Fullerton Philanthropic Foundation (Foundation) cost allocation analyses for fiscal years 2006/07 and 2007/08 had not been signed and dated evidencing campus CFO approval of post-year calculations.

› The Associated Students California State University, Fullerton, Inc. (AS) cost allocation analysis for fiscal year 2007/08 had not been completed, and the analysis for fiscal year 2006/07 had not been signed and dated evidencing campus CFO approval of post-year calculations.

The Corporation Indirect Cost Allocation Plan states that cost allocation calculations will be approved and dated by the associate vice president of finance on an annual basis.

Executive Order (EO) 753, Allocation of Costs to Auxiliary Enterprises, dated July 28, 2000, requires that an annual written cost allocation plan is prepared to ensure that auxiliary enterprises are charged for allowable direct costs plus an allocable portion of indirect costs associated with facilities, goods, and services provided by the university, funded from the operating fund. Cost allocations shall be determined in accordance with a written cost allocation plan approved annually by the campus CFO.

The campus associate vice president of finance stated that most cost analyses had been completed; however, the need to formally document these analyses, including approval signatures and dates, even when an auxiliary does not owe money, had not been clearly communicated to the various financial services staff preparing the analyses. He added that the lack of a documented AS cost allocation analysis for fiscal year 2007/08 was due to oversight.

Failure to timely complete and approve the cost allocation plan increases the risk that the campus-operating fund will not be fully compensated for support provided to auxiliary enterprises.
Recommendation 1

We recommend that the campus ensure that annual auxiliary cost allocation analyses are completed timely and formally approved, with signature and date, by the campus CFO or his designee.

Campus Response

We concur. All auxiliary cost allocation analyses identified above were signed and dated by the associate vice president of finance during audit fieldwork and remain current. Future annual auxiliary cost allocation analyses will be completed timely and formally approved, with signature and date, by the associate vice president of finance.

INFORMATION TECHNOLOGY

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

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

We found that:

- Roles and responsibilities for PCI compliance were not adequately defined.

- A compliance risk assessment was not performed to determine comprehensive compliance obligations for credit card data maintained on auxiliary servers and transmitted throughout the campus network as required by PCI DSS.

- An annual PCI DSS Self-Assessment Questionnaire (SAQ) was not completed.

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

The PCI DSS is a set of comprehensive requirements for enhancing payment account data security, which was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. According to payment brand rules, all merchants and their service providers are required to comply with the PCI DSS in its entirety.
The PCI DSS SAQ is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. The PCI DSS SAQ consists of the following two components: (1) Questions correlating to the PCI DSS requirements, appropriate to service providers and merchants; and (2) An attestation of compliance which attests to an organization’s certification of eligibility to perform and have performed the appropriate self-assessment.

The campus chief information officer (CIO) stated that the campus was aware of PCI DSS requirements and had made significant progress towards PCI DSS compliance since the August 2008 Information Security audit, including determination of the campus’ applicable vendor level and specific requirements, but had not fully addressed the collective union of campus and auxiliary roles and responsibilities for PCI DSS assessment.

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

**Recommendation 2**

We recommend that the campus and auxiliaries:

a. Define and document roles and responsibilities for PCI compliance between the campus and auxiliaries.

b. Conduct a risk assessment of comprehensive compliance obligations for credit card data maintained on auxiliary servers and transmitted throughout the campus network.

c. Complete an annual SAQ to include all credit card merchants on campus, whether completed jointly or separate from the auxiliaries.

**Campus Response**

We concur.

a. The campus has developed a standard for the acceptance of credit cards which defines administrative, technical, and user roles and responsibilities and establishes centralized processes for reviewing all organizational requests for accepting credit cards.

b. The information security office annually conducts a Protected Data survey across all campus divisions. The developed *University Standard for the Acceptance of Credit Cards* specifically states, “The Information Security Office will perform a yearly risk assessment of comprehensive compliance obligations for credit card data maintained on all campus and auxiliary servers which transmit data throughout the campus network. The assessment will be the principle tool used to complete the required PCI self-assessment.” The 2009-10 Protected Data survey will be completed by December 23, 2009.
c. The Corporation, AS, Foundation, and the campus have completed the 2008-09 annual SAQ assessment and have either retained this assessment for the record or have forwarded the assessment to the respective acquirer, as specified by the acquirer.

**USER ACCESS REVIEWS**

The Corporation, Foundation, and AS did not perform periodic, documented management reviews of user access privileges within all 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 California State University (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 executive directors of these auxiliaries stated that management reviews of user access privileges were completed on an informal ad hoc basis, but were not consistently documented. The executive directors further stated that they were unaware of the requirement to periodically document management reviews of user access privileges.

Failure to periodically perform a documented review of user access to systems containing protected data increases the risk of inappropriate access.

**Recommendation 3**

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

**Campus Response**

We concur. The Corporation and the Housing Authority will conduct annual documented management reviews of user access for all systems containing protected data. The review for year 2009-10 will be completed by September 30, 2009. AS has implemented a policy to perform periodic documented management reviews of user access privileges within the critical systems and
those systems containing protected data. This review was performed in September 2009 and will be performed on an annual basis. The Foundation will conduct annual documented management reviews of user access for all systems containing protected data by June 30 of each year. The review for year 2009-10 was completed on June 30, 2009.

INFORMATION SECURITY TRAINING

Corporation, Foundation, and AS personnel with access to protected data were not required to complete information security awareness training.

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

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

The campus CIO stated that the auxiliaries had implemented some forms of employee education regarding information security policies and requirements, although this may not have provided comprehensive coverage of information security risks. He added that instead of focusing on the training program of each auxiliary, resources were instead directed to the Workplace Answers module for information security awareness training that was made available to, and required of, all campus and auxiliary employees on March 17, 2009.

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 4

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

Campus Response

We concur. The auxiliaries will develop and implement an action plan by November 5, 2009.
CSU FULLERTON AUXILIARY SERVICES CORPORATION

OPERATING AND ADMINISTRATIVE AGREEMENTS

Certain business arrangements between the CSU Fullerton Auxiliary Services Corporation (Corporation) and third parties were not supported by complete and/or current written agreements.

We found that:

- An agreement with a laundry service provider expired on June 30, 2004, and had not been renewed. In addition, the indemnification provision did not specifically indemnify the CSU Trustees, the campus, and the State of California.

- An agreement with a vending machine service provider expired on July 31, 2004, and had not been renewed.

- An agreement with a credit union for automated teller machine service expired on June 30, 2006, and had not been renewed.

- An agreement with a food service vendor expired on May 1, 2008, and had not been renewed.

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.

The Corporation controller stated that the agreements had not been renewed due to the lack of a mechanism for tracking contract expiration dates. He further stated that the absence of an appropriate indemnification provision was due to oversight.

The absence of current written agreements and an appropriate indemnification provision increases the risk of misunderstandings and miscommunication regarding rights and responsibilities and subjects the auxiliaries and CSU to potential liability.
Recommendation 5

We recommend that the Corporation:

a. Promptly renew the agreements with the noted service providers.

b. Implement a process to ensure that all future agreements are timely renewed and include an appropriate indemnification provision.

Campus Response

We concur. The Corporation has renewed the agreements with the noted service providers and implemented a process to ensure that all future agreements are timely renewed and include an appropriate indemnification provision.

CORPORATE GOVERNANCE

The Corporation did not have the required number of community directors on its governing board for fiscal years 2006/07, 2007/08, and 2008/09.

We found that the Corporation board had one community director vacancy for fiscal year 2006/07 and two vacancies for fiscal year 2007/08. Further, the Corporation had not yet filled the vacancies for fiscal year 2008/09.

The Corporation Bylaws, Article V §4(d) requires eight community directors to assume positions as board members effective January 1st in alternative years.

Title 5 §42602 (b) specifically requires community representation on auxiliary organization boards.

The Corporation executive director stated that proper board representation was not maintained due to difficulties in recruiting community members.

Failure to maintain mandated board composition violates statutory requirements and increases the risk that all views will not be adequately represented.

Recommendation 6

We recommend that the Corporation ensure that appropriate board representation is maintained.

Campus Response

We concur. The Corporation will ensure appropriate board representation is maintained by October 31, 2009.
OPERATIONAL COMPLIANCE

The Corporation did not track the transfer of inventory from the bookstore centralized receiving dock to satellite locations.

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 procedures to address inventory transfer.

The Corporation controller stated his belief that the Corporation had sufficient controls over bookstore inventory. He added that one inventory system was used for the main shop and shops located at satellite locations.

The absence of documented inventory transfers increases the risk of errors or misappropriation.

Recommendation 7

We recommend that the Corporation develop and implement written procedures to address the transfer of inventory from the bookstore centralized receiving dock to satellite locations. Such procedures should include documentation of inventory quantity and type transferred, handling of inventory transferred, safeguards over inventory in transit, and acknowledgement of receipt of inventory transferred.

Campus Response

We concur. The Corporation will develop procedures to address the transfer of inventory from the bookstore centralized receiving dock to satellite locations, including documentation of inventory quantity and type, inventory transfer handling, safeguards during transit, and acknowledgement of receipt by October 31, 2009.

PROGRAM COMPLIANCE

The Corporation had neither established nor implemented a process to report to the campus financial aid office stipends paid to student interns working for the Titan Daily newspaper.

We found that for the period January 1, 2008, through December 31, 2008, the Corporation paid stipends totaling $107,515 to 52 students. However, these payments were not reported to the campus financial aid office.
Title 5 §42500(d) states that a record of financial assistance, such as student loans, scholarships, stipends, and grants-in-aid shall be forwarded on a timely basis to the campus financial aid office and shall be documented on student financial aid recipient records in that office.

The Corporation executive director stated that the Corporation was unaware of the requirement to report stipends to the campus financial aid office.

Failure to report student intern stipends to the campus financial aid office may result in an overpayment of financial aid funds and increases the risk of fines and penalties.

**Recommendation 8**

We recommend that the Corporation establish and implement a process to report all student intern stipends to the campus financial aid office.

**Campus Response**

We concur. The Corporation will develop and implement a process to report all student intern stipends to the campus financial aid office by October 31, 2009.

**CASH RECEIPTS AND HANDLING**

The Corporation had not developed written policies and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery.

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 proper administration of cash shortages and/or overages.

The Corporation controller stated his belief that present mitigating controls were considered sufficient and cash shortages were not a significant risk.

The absence of written policies and procedures to address cash shortages and/or overages increases the risk of loss or misappropriation of funds.
Recommendation 9

We recommend that the Corporation develop written policies and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery.

Campus Response

We concur. The Corporation will develop written policies and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery by October 31, 2009.

TRUSTS AND OTHER LIABILITIES

Certain campus program revenues were inappropriately deposited to, and held in custody by, the Corporation.

The Corporation financial statements as of June 30, 2008, indicated that the Corporation administered and maintained 116 custodial trust accounts totaling $4,217,414 for campus programs, departments, colleges, and other groups. Our review of 15 of those accounts disclosed that state funds were being inappropriately held by the corporation.

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

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

The Corporation controller stated that a review of custodial trust accounts had been initiated to determine whether any state funds were being inappropriately held but had not yet been completed due to resource constraints.

The campus’ required oversight of state funds is limited when funds are deposited outside the custody of the CFO.
Recommendation 10

We recommend that the Corporation:

a. Complete a review of all custodial trust accounts reflected as “deposits held for others” on its financial statements and determine, within 60 days, which accounts contain state funds.

b. Submit to the Office of the University Auditor, within 60 days, a list of those custodial trust accounts which have been deemed appropriate to remain in the custody of the Corporation and comprehensive documentation to support the sources of funds for those trust accounts.

c. Move those state funds identified in “a” above to campus accounts within six months.

Campus Response

We concur. The campus will complete a review of all custodial trust accounts and submit to the Office of the University Auditor by November 10, 2009, a list of those accounts deemed appropriate to remain in the custody of the Corporation and comprehensive documentation to support the sources of funds for those trust accounts. Any state funds identified will be moved to campus accounts within six months.

AUXILIARY PROGRAMS

Cost share and effort certification reports were not always prepared at the Corporation.

Our review of ten sponsored project files disclosed that:

- Both grants with cost sharing requirements lacked completed cost share certification reports.
- Three of six federal grants reviewed lacked completed effort certification reports by faculty.

The Corporation Principal Investigator Reference Manual states that requests for cost sharing documentation will be made to the principal investigator each quarter. Sponsored programs will provide forms and suggestions for adequate cost sharing documentation. The “certification of cost share” report is the means of tracking and documenting the cost share obligations.

The Corporation Sponsored Programs Policies and Procedures for Effort Certification states that effort certification must be included with every time sheet submitted for staff and non-professorial employees. The office of sponsored programs will distribute faculty effort reports to the project director on each account at the end of each semester.

Office of Management and Budget (OMB) Circular A-110, Uniform Administrative Requirements for Grants and Agreements With Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations, §.51(a), indicates that recipients are responsible for managing and monitoring each project, program, sub-award, function, or activity supported by the award.

Auxiliary Organizations/California State University, Fullerton/Audit Report 09-13
Page 21
EO 890, *Administration of Grants and Contracts in Support of Sponsored Programs*, dated January 7, 2004, 3.5.5 *Cost Sharing*, states that when there is cost sharing or matching in connection with a sponsored program, the sponsored program administrator, in conjunction with the principal investigator, must document actual costs shared or matching contributions in a manner consistent with the campus cost allocation plans, sponsor requirements, and in the case of federal contracts and grants requirements as stated in OMB Circular A-110.

The Corporation director of sponsored programs stated that cost sharing requirements were informally recorded for one grant through the use of a “request for reimbursed release time” form and were recorded for the other grant through the use of budget justification spreadsheets and both had been booked against the general ledger. She further stated that effort certification reports were sent to principle investigators at the end of each semester, but the reports were not consistently completed and timely returned to the office of sponsored programs.

Failure to complete cost share and effort certification reports increases the risk of reduced reimbursements, non-compliance with OMB requirements, and increased regulatory scrutiny.

**Recommendation 11**

We recommend that the Corporation reiterate to staff cost share and effort certification requirements and implement a process to ensure the completion of cost share and effort certification reports.

**Campus Response**

We concur. The Corporation will reiterate to staff cost share and effort certification requirements and will work with the university to implement a process to ensure the completion of cost share and effort certification reports by October 31, 2009.

**INFORMATION TECHNOLOGY**

**PASSWORD SECURITY**

Password controls and security parameters were not always adequate for Corporation systems.

We found that:

- Password files were not adequately protected from unauthorized access by ordinary users, as a shadow password file for the Integrated Financial Accounting System (IFAS) accessed via the UNIX operating system was not in place. This is a repeat finding from the prior auxiliary organizations audit.

- The minimum password length for access to the Missouri Book System (MBS) and IFAS (via UNIX) was six characters instead of the minimum eight characters required by campus password guidelines.
California State University, Fullerton (CSUF) *Account and Password Guidelines* recommend that all systems require a minimum of eight characters for passwords. It also states that all user-level and system-level passwords must conform to the guidelines.

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 controls over access to password files and password parameters.

The Corporation director of management information systems (MIS) stated that the IFAS and MBS shadow password implementation was scheduled as the final step of a coordinated project that included a major operating system upgrade and patch and program installation. He added that the other password parameter deficiencies were due to oversight.

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

**Recommendation 12**

We recommend that the Corporation:

a. Implement a shadow password file for the IFAS.

b. Set effective password security parameters for the MBS and IFAS in accordance with campus guidelines and perform an assessment of password security parameters for all other Corporation systems.

**Campus Response**

We concur. The IFAS server is now running in HP-UX Trusted Mode, allowing the system to run at C-2 level security, store passwords in an encrypted database, and assign a minimum password length of eight characters. Password security parameters have been established in accordance with campus guidelines for MBS, IFAS, and all other Corporation systems.
PROTECTED DATA ASSESSMENT AND SECURITY

The Corporation had not adequately secured certain systems and files containing critical and/or sensitive data, nor performed an assessment and inventory of protected data residing on an administrative file server.

We found that:

- The IFAS financial and payroll systems that contained critical data and protected employee data were not encrypted, although the server on which they resided was behind a demilitarized zone (DMZ).

- The “payroll records super directory” server that contained protected employee data was not encrypted and did not reside behind a DMZ, which resulted in an increased risk of internal network exposure to security compromises from its location on the same network segment as Internet-accessible devices (web servers). Further, the “payroll records super directory” file transfer protocol (FTP) files were sent over the network to the university payroll office without encryption.

- An administrative file server with shared drives for administrative, accounting, and sponsored programs was not encrypted, and an assessment and inventory of protected data had not been conducted such that the existence of protected data was unknown. In addition, this server was stored in the MIS director’s office (outside of the Corporation data center) without adequate physical and environmental security. Further, the server did not reside behind a DMZ, which resulted in an increased risk of internal network exposure to security compromises from its location on the same network segment as Internet-accessible devices (web 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.

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 protection and encryption of any protected data residing on auxiliary systems and/or in files, as well as periodic assessment and inventory of protected information residing on systems.

The Corporation MIS director stated that the IFAS systems used for the financial and payroll functions were programmed, released, and supported by a third-party vendor, such that additional encryption added without vendor support and approval may have caused the applications to stop functioning properly. He also stated that the unencrypted storage of payroll files and transfers between the Corporation and the campus was due to oversight. He further stated that the
administrative file server access functions were a recent addition and were temporarily located in the office during testing since the server provided very limited access to protected information.

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

**Recommendation 13**

We recommend that the Corporation:

a. Properly secure all systems and servers containing critical and protected data.

b. Encrypt the storage and transfer of payroll files contained within the “payroll records super directory.”

c. Perform an assessment and inventory of protected data on all Corporation servers, including administrative file servers, to determine the existence of any protected data and the need for appropriate logical and physical security measures.

**Campus Response**

We concur. All systems and servers containing protected data are now located in the computer center behind a NetScreen firewall administered by the university’s information technology division, and stored and transferred payroll records files are now encrypted. An inventory and assessment of protected data on Corporation servers to determine the need for additional security measures is in progress and will be completed by October 31, 2009.

**DATA CONFIDENTIALITY FORMS**

Corporation personnel with access to critical systems and 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 data confidentiality forms prior to being granted access to auxiliary systems.
The Corporation MIS director stated that the Corporation had not required the completion of data confidentiality forms because it was unaware of this requirement.

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

**Recommendation 14**

We recommend that the Corporation:

a. Establish a policy requiring data confidentiality forms from all employees prior to granting them access to critical systems and protected data.

b. Obtain completed forms from personnel who currently have access to such data.

**Campus Response**

We concur. The Corporation has adopted the university’s policy requiring confidentiality forms from all employees prior to granting access to protected data. Obtaining completed forms from personnel who currently have access to such data was completed in conjunction with the systemwide information security training initiated in March 2009.

**SYSTEM BACKUPS**

Backups for Corporation systems were not adequately controlled.

We found that:

- Daily and weekly backups for Corporation systems with protected data were not encrypted when stored locally or when in transit to the bookstore via the bookstore warehousing transport.

- Backup tapes were not deposited into the bookstore safe immediately upon return to the bookstore, but were sometimes held in the warehouse until the next day.

- The Corporation had not contracted with any off-site backup storage facility for disaster recovery purposes, but instead all backups were stored on campus (either locally or at the bookstore).

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 and off-site storage for disaster recovery purposes.

The Corporation MIS director stated that he was unaware of the need to encrypt Corporation backups during transport or to establish an off-campus storage location. He also stated that securing backup tapes in the bookstore safe immediately after transport was common practice and that tapes remaining overnight in the warehouse was rare.

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, while inadequate storage increases the risk that auxiliary systems will not be recovered in the event of a disaster.

**Recommendation 15**

We recommend that the Corporation:

a. Encrypt system backups with protected data.

b. Strengthen procedures to ensure that the transfer to, and storage of, backups at the bookstore are adequately controlled.

c. Evaluate the security benefits of contracting with an off-campus backup storage facility, including the opportunity to merge backup processes with the campus.

**Campus Response**

We concur. The Corporation will work with the university to evaluate mechanisms of encrypting backups with protected data by December 31, 2009, and has already contracted with an off-campus backup storage facility to ensure backup transfer and storage is adequately controlled.

**REMOTE SERVER ACCESS**

Remote access to Corporation servers was not always secure.

Telecommunication Network (Telnet), an unsecure remote access protocol that allows users to connect to remote computers and transmits data in clear text, was enabled on the MBS and IFAS application servers to permit remote access by the vendor (through an opened port/firewall pinhole) for performing system updates.

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 Corporation MIS director stated that Telnet was utilized exclusively by a third-party vendor to provide support services approximately 10 to 12 times per year and requires the vendor to log into the secure campus virtual private network (VPN) system.

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 that 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 16**

We recommend that the Corporation 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 VPN connection has been established.

**Campus Response**

We concur. The Corporation will work with the university to enforce internal firewall restrictions on Telnet such that it can only be accessed once a VPN connection has been established by December 31, 2009, or replace Telnet remote access with a more secure remote access protocol (such as secure shell).

**DISASTER RECOVERY PLAN**

The Corporation had not completed a written information technology disaster recovery plan.

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 computer operations, including backup and recovery mechanisms and disaster recovery programs.

The Corporation MIS director stated that a draft disaster recovery plan was in progress but had not been completed prior to the audit due to other priorities and limited resources.
Without a detailed, written information technology disaster recovery plan, business operations may be interrupted and data processing operations may not be restored within a reasonable time frame.

**Recommendation 17**

We recommend that the Corporation complete a written information technology disaster recovery plan.

**Campus Response**

We concur. A written information technology disaster recovery plan is now complete and will be officially adopted by the Corporation by October 31, 2009.

**ENVIRONMENTAL CONTROLS**

The Corporation data center had a water-sprinkler system which could be detrimental to the electrical equipment housed in the data center, and several of the servers were not elevated above the floor in the event of flooding.

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

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

The Corporation MIS director stated that an alternative to the water-sprinkler equipment had been considered but was not implemented due to cost constraints. He also stated that older servers housed in the data center had been elevated; however, several newer servers recently added to the data center had not yet been elevated.

Failure to maintain appropriate fire suppression devices and flood mitigation controls in the data center increases the risk of unsuccessful suppression of a fire and/or damage to critical systems, which may expose employees to dangerous conditions and may result in the loss of critical systems.

**Recommendation 18**

We recommend that the Corporation evaluate the feasibility of another means of fire suppression other than water sprinklers or implement mitigating controls to ensure that all servers are not damaged from any resulting flooding.
Campus Response

We concur. The Corporation will work with the building property manager to evaluate the feasibility for another means of fire suppression other than water or implement to ensure all servers are protected from potential fire system water damage by November 30, 2009.
CSU FULLERTON PHILANTHROPIC FOUNDATION

FISCAL COMPLIANCE

The CSU Fullerton Philanthropic Foundation (Foundation) had not developed a written reserve policy.

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, 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.

The Foundation CFO stated that although an operational reserve was in place as of July 1, 2006, an operational reserve policy had not been adopted by the board of governors.

The absence of reserve planning and analysis increases the risk that the auxiliary will be unable to fund future needs.

Recommendation 19

We recommend that the Foundation develop a written reserve policy to address the allocation of surplus funds/reserves. Such a policy should address minimum reserve requirements, board review of reserve levels, reserves for working capital and capital replacement, and the methodology used for the calculation of reserves.

Campus Response

We concur. A reserve policy was adopted by the Foundation board of governors on May 1, 2009. The policy among other things addresses the allocation of surplus funds/reserves.

OPERATIONAL COMPLIANCE

The Foundation had not developed a written risk management policy.

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 Foundation CFO stated that the Foundation did not have employees or physical assets, and investment risks were considered in the approved Investment Policy; therefore, a formal risk management policy had not been considered.

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

**Recommendation 20**

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

**Campus Response**

We concur. The Foundation is preparing a draft risk management policy. The draft policy will be presented to the board of governors for adoption by February 26, 2010.

**FEES, REVENUES, AND RECEIVABLES**

Storage of donation forms and documentation containing credit card information from donors was not in compliance with PCI standards at the Foundation.

We found that credit card information (full card number, three-digit security code, expiration date, cardholder name and address) was collected via four different processes and stored in unencrypted formats on the FileNet document imaging system and the SmartCall telemarketing system.

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

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 sensitive information should be properly safeguarded to prevent unauthorized access.

The Foundation CFO stated that the credit card data was stored in these systems for operational efficiency when donors requested to make repeat donations from their credit cards on file. He further stated that the Foundation was unaware that these systems were not enabled with encryption controls. Insufficient control over access to sensitive donor information increases the risk of unauthorized and inappropriate acts.

**Recommendation 21**

We recommend that the Foundation ensure that donor credit card information is stored in compliance with PCI standards and that safeguards be implemented to ensure that protected data is adequately secured.

**Campus Response**

We concur. The Foundation, in coordination with the office of university advancement, redacts written credit card information. Credit card information is no longer stored on the FileNet system. The SmartCall telemarketing system uses encrypted technology.

**ENDOWMENT ADMINISTRATION**

Certain Foundation endowment files lacked executed endowment agreements, and some endowment agreements did not delineate management fees and/or the annual spending policy.

Our review of 15 endowment files disclosed that:

- In three instances, endowment files did not contain fully executed endowment agreements.
- In 11 instances, endowment agreements did not address the Foundation’s management fees.
- In four instances, endowment agreements did not address the Foundation’s annual spending policy.

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 Foundation CFO stated that the advancement staff was advised to use an endowment gift agreement template when presenting endowment proposals to donors, but this was not always done. He added that the template considered distribution methodology, but did not adequately address management fees or the annual spending policy.

Recommendation 22

We recommend that the Foundation:

a. Implement a process to ensure the establishment and execution of endowment agreements.

b. Revise its endowment agreement to specifically address the Foundation’s management fees and annual spending policy.

Campus Response

We concur.

a. The Foundation will advise all directors of development and university advancement fundraising personnel of the requirement for review of draft endowment agreements by the Foundation CFO prior to the submission to potential donors. Endowment agreements are not fully executed until approved and signed by the vice president for university advancement and the Foundation CFO.

b. The Foundation has revised its endowment agreement to include explanations of the endowment management fee and the annual spending policy.

INFORMATION TECHNOLOGY

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

The Advance donor system restricted reuse of the current password, but it did not enforce password history any further, and there was no minimum time enforcement between password changes. The combination of these two settings allows users to quickly recycle their passwords in order to effectively circumvent the password expiration controls.

CSUF Account and Password Guidelines recommends that changed passwords be remembered 24 times and not be re-used. It also states that all user-level and system-level passwords must conform to the guidelines.
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 university advancement director of information services stated her belief that the existing password settings were considered adequate and, therefore, increased password security was unnecessary.

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

**Recommendation 23**

We recommend that the Foundation reassess its security requirements and set effective password security controls for its computer systems.

**Campus Response**

We concur. The Foundation information technology security requirements will be reassessed in coordination with the scheduled upgrade to an Oracle platform. The Foundation will also reassess password security controls after Oracle implementation is completed on December 31, 2009.
ASSOCIATED STUDENTS
CALIFORNIA STATE UNIVERSITY, FULLERTON, INC.

FISCAL COMPLIANCE

Unrelated business income (UBI) for the Titan Bowl and Billiards was not properly accounted for/reported by Associated Students California State University, Fullerton, Inc. (AS).

AS had not accounted for or tracked UBI for Titan Bowl and Billiards services provided to community members. Titan Bowl and Billiards revenues were not included in the Internal Revenue Service (IRS) Form 990T for 2006 and 2007.

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

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

The AS executive director stated that UBI for Titan Bowl and Billiards was not previously reported because accounting was unaware of the increase in services provided to the community.

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

Recommendation 24

We recommend that AS account for and track UBI for Titan Bowl and Billiards services provided to community members, and file federal income tax returns as appropriate.

Campus Response

AS will engage our external auditor to thoroughly review all operations and types of revenue for an official opinion on revenue types to be reported as unrelated business activity. AS will comply with the independent auditor’s recommendation for future tax reporting. We anticipate that we will have a response from our external auditor by October 2009 and will proceed accordingly.
CASH RECEIPTS AND HANDLING

The transfer of AS cash receipts was not adequately documented and safeguarded.

We found that:

▶ Funds for deposit were transferred from AS units (Children’s Center, Conference Center, Information Services, Titan Bowl and Billiards, and the Student Recreation Center) to the AS central cash vault without the use of transfer receipts.

▶ Deposits were walked across campus to the AS central cash vault by a single employee and there was no policy for the use of two employees or a public safety escort in the event of large deposits.

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 AS executive director stated his belief that the existing policies and procedures were adequate.

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

Recommendation 25

We recommend that AS:

a. Implement the use of transfer receipts when funds are transferred between locations.

b. Establish a written policy for the transport of deposits between locations and increase cashiers’ awareness of the availability of security escorts when deposits are transferred from outlying areas and in the event of large deposits.
Campus Response

We concur.

a. A transfer receipt will be utilized when funds are transferred between locations. We are in the process of implementing a standard transfer receipt/transfer log to be used by all departments. This will be completed by November 2009.

b. We have implemented a policy to specify that when $3,000 or more in cash (currency and coin) is being transported from the central cash vault to any AS department, or from any AS department to the central cash vault, cash will be transported by two people or by utilizing the services of a public safety escort. A Cash Transport Policy was drafted and implemented in April 2009.

FEES, REVENUES, AND RECEIVABLES

Administration of AS delinquent accounts receivable required improvement.

We found that:

› Collection activity and follow-up on past-due agency and third-party accounts receivable were not adequate to ensure collection. Our review of delinquent accounts receivable as of January 31, 2009, disclosed that AS had not documented collection correspondence at sufficient intervals (30, 60, and 90 days) and did not address further action to be taken on delinquent accounts.

› Policies and procedures had not been documented for the monitoring of accounts receivable, collection of delinquent agency accounts and third-party receivables, and bad debt write-offs.

The Compilation of Policies and Procedures for California State University Auxiliary Organizations sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.4, Receivables, states that the auxiliary should establish a written system to invoice customers promptly, in a consistent manner, while exercising due diligence in the follow-up and collection of past-due accounts.

The AS accounting manager stated his belief that the existing policies and procedures were adequate, and since most accounts receivable were between the AS and the university, the risk of loss was minimal.

Inadequate control over accounts receivable increases the risk that receivables will not be properly controlled and reflected in auxiliary financial statements, reduces the likelihood of collection, and negatively impacts cash flow.
Recommendation 26

We recommend that AS:

a. Formally document collection activity of delinquent accounts receivable in order to facilitate collection or to support write-off.

b. Establish and implement written policies and procedures for the monitoring of accounts receivable, the collection of delinquent agency accounts and third-party receivables, and bad debt write-offs.

Campus Response

We concur. AS has implemented policies and procedures addressing the process and documentation of collection activity and/or write-off of past-due accounts. A Collection of Past Due Accounts policy was drafted and implemented in June 2009.

PURCHASING AND ACCOUNTS PAYABLE

Certain AS cash disbursements were neither supported by sufficient and appropriate documentation nor appropriately authorized. The processing exceptions were all repeat findings from the prior auxiliary organizations audit.

Our review of 44 cash disbursements disclosed that:

Process Controls

› Agency accounts and athletic department disbursements were not processed in accordance with AS accounts payable procedures. Specifically, we noted that AS did not scrutinize supporting information submitted for withdrawals or reimbursements. For example, AS granted a $300,000 line of credit to the athletic department and indicated that it did not apply its internal policies and procedures to disbursements for this line of credit.

Processing Exceptions

› In 15 instances, AS did not obtain proper supporting documentation. Specifically, disbursements were supported by photocopies of original receipts, duplicate copies of invoices, credit card slips, quotes, and bids. Although AS required the employee to stamp, sign, and certify the photocopies submitted for reimbursement, documentation was not provided to evidence that this process was monitored or reviewed for excessive or repeat offenses.

› In seven instances, payment was issued without an approved travel request.

› In seven instances, payment was issued without an approved requisition or purchase order.


AS Business and Financial Policies and Procedures Section 3.1, Agency Accounts; Deposits and Withdrawals, states that the agency account check request should be completed in full, including “date of request,” payee “name and address,” and a phone number of an individual to contact regarding the check request. Check requests should be validated when submitted to the accounting office. The signatures on the check requests must agree with the signatures on the agency account form, the account balance must be sufficient to cover the check request amount, and check requests should be returned to the submitter if the signatures do not match or the account has insufficient funds. It further states that supporting documentation requires original receipts or invoices. Copies or faxes of receipts or invoices, credit card slips, automated teller machine slips, or Internet printouts are not considered valid supporting documentation and require a certification that the document is being submitted as an original and will not be submitted elsewhere for payment. It also states that when requesting reimbursement for completed airline travel, a boarding pass or airline ticket is required as supporting documentation.

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 cash disbursements be fully supported and properly authorized.

The AS accounting manager stated that these accounts are considered agency funds, which are kept but not controlled, and the AS accounting staff operated under the assertion that fiduciary responsibility remained with the student organizations and departments.

Insufficient supporting documentation and/or lack of appropriate authorization increase the risk of errors, irregularities, and misappropriation of funds.

Recommendation 27

We recommend that AS:

a. Enforce accounts payable procedures to ensure that agency accounts and athletic department disbursements are processed in accordance with AS accounts payable procedures.

b. Reiterate to staff existing cash disbursement policies and procedures regarding sufficient and appropriate supporting documentation and authorization.
Campus Response

We concur.

a. We will process AS disbursements in compliance with our accounts payable procedures and will revise AS policies and procedures to clarify our practice with regard to funds held for others, specifically agency and athletics accounts. We revised our Agency Accounts policy effective August 2009. We also implemented an Athletics Accounting policy effective August 2009. We will revise our accounting services agreement with athletics to reflect these policies by November 2009.

b. AS has cash disbursement policies and procedures in place that outline appropriate supporting documentation and authorization. These were distributed in June 2009 to every department and program AS funds as part of the annual budget process for fiscal year 2009-10. As a follow-up, we will send out a notice each semester reminding staff of the need for strict compliance with these budget policies and procedures.

INFORMATION TECHNOLOGY

PASSWORD SECURITY

Password security parameters were not always adequate for AS systems, and system administrators were unable to review and change security parameters for several critical systems.

We found that:

- The minimum password lengths for access to the Counterpoint and IFAS systems were three and six characters, respectively, instead of the minimum eight characters required by campus password guidelines.

- System administrators were unable to review and change the password and login security parameters for several of the critical systems with protected data.

CSUF *Account and Password Guidelines* recommend that all systems require a minimum of eight characters for passwords. It also states that all user-level and system-level passwords must conform to the guidelines.

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 as well as adequate management and administration of system security.

The AS executive director stated that the Counterpoint system was utilized with default vendor-established parameters that were assumed to be adequate and the IFAS system parameters were controlled by the Corporation. He added that the responsibilities of AS system administration, specifically for password and login security parameters, were not adequately communicated throughout AS.

Inadequate password parameters and system security administration may compromise the authentication credentials of user account privileges that are embedded into applications and operating systems and result in other security deficiencies; all of which increase the risk of unauthorized access to auxiliary systems and confidential data.

**Recommendation 28**

We recommend that AS:

a. Reassess its security requirements and set effective password security controls for Counterpoint and IFAS systems in accordance with campus guidelines and perform an assessment of password security parameters for all other AS systems.

b. Clarify and document the security responsibilities of systems administrators, specifically for password and login security parameters.

**Campus Response**

We concur. The application administrators have been trained to review and change the password and login security parameters for all critical systems with protected data. This training took place in July 2009. The systems administrator will periodically review login security parameters for all critical systems with protected data. This was accomplished in August 2009 and will be reviewed annually. With regard to password character lengths, we will now enforce the use of 8-character password lengths for all systems (effective July 2009).

**ENVIRONMENTAL CONTROLS**

The AS server room lacked fire or smoke detection devices, although a fire extinguisher was located within the room.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.
Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that appropriate fire and smoke detection equipment be maintained within the premises of server/data centers at all times.

The AS executive director stated that the installation of fire detectors was not considered necessary at the time the server room was established.

Failure to maintain appropriate fire and smoke detection devices in the server room increases the risk of untimely fire notification, which may expose employees to dangerous conditions and increases the risk of catastrophic loss of computing equipment and data processing capability.

**Recommendation 29**

We recommend that AS implement a fire and smoke detection system in the server room.

**Campus Response**

We concur. We have installed a smoke detector in the AS data center.
CSU FULLERTON HOUSING AUTHORITY

CORPORATE GOVERNANCE

The CSU Fullerton Housing Authority (Housing Authority) had not filed amended Articles of Incorporation with the chancellor’s office in a timely manner.

We found amendments to the Articles of Incorporation made on July 23, 2007, and submitted to and approved by the Secretary of State on August 4, 2007, that had not been filed with the chancellor’s office.

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 11.6.1, Reporting Changes in Articles of Incorporation (or Constitutions) and Bylaws, states that when the 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 Housing Authority executive director stated that the amended Articles of Incorporations were submitted to the chancellor’s office at the time the amendments were approved, but could not furnish proof of submission.

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

Recommendation 30

We recommend that the Housing Authority promptly file the cited amendments with the chancellor’s office and develop a procedure to ensure that all future changes/amendments to Articles of Incorporation are timely filed with the chancellor’s office.

Campus Response

We concur. The cited amendments were resubmitted to the chancellor’s office in March 2009, and a procedure was developed to ensure that all future amendments to Articles of Incorporation are submitted timely and a record of these submissions is maintained in Housing Authority files.
SEGREGATION OF DUTIES

Certain duties and responsibilities related to cash receipts processing were not adequately segregated at the Housing Authority.

We found that one employee:

- Handled checks received through the mail.
- Endorsed the checks.
- Prepared an accounting ledger in Excel for posting.
- Prepared the deposit and delivered it to the bank.
- Performed bank reconciliations without independent review.

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 establish a written internal controls system that ensures cash receipts and disbursements are conducted with appropriate segregation of duties.

The Housing Authority executive director stated that duties related to cash receipts processing were not properly segregated due to oversight.

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

Recommendation 31

We recommend that the Housing Authority appropriately segregate certain cash receipts processing functions or institute mitigating procedures approved by the campus CFO.

Campus Response

We concur. Cash receipts processing has been appropriately segregated.

PURCHASING AND ACCOUNTS PAYABLE

Housing Authority oversight of purchasing activities performed by a third-party property management firm for University Gables and University Heights, as well as the reimbursement of activities performed by a real estate agent, were not adequate.
We found that:

- The written agreement with the property management firm required that the firm establish an annual budget for operating expenses associated with University Gables and University Heights employee housing. During the year, the property management firm was contracted to collect revenues and procure goods and services for the housing operations. The Housing Authority subsequently reviewed these transactions based on accounting data submitted by the property management firm and then input the data into the Housing Authority accounting system for posting. This review consisted of comparing transaction line items for goods and services procured to what was originally budgeted, but did not include the review of supporting vendor invoices.

- A residential listing agreement with a real estate agent for an initial period of six months stated that the agent would cover all marketing costs associated with the sale of the University Heights employee housing units, and that the agent would also cover the costs of staging a model home if the listing agreement was extended an additional six months. The agreement stated that if the Housing Authority chose not to extend the agreement for the additional six months, then the costs of staging the model home would be reimbursed to the agent up to the amount of $5,000. This agreement was cancelled prior to the completion of the additional six-month period, so the agent submitted a list of expenses to be reimbursed, including a general charge for staging and marketing of $5,000, as well as specific costs not stated within the agreement such as painting, cleaning, and staging beyond additional listing for an additional $3,828. The Housing Authority paid the total $8,828 of costs requested by the agent for this University Heights listing agreement as well as $877 of other expenses requested for reimbursement by the agent for the Creekside property without a review of actual invoices or receipts.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.5, *Procurement*, states, in part, that the auxiliary should establish a written system that provides for purchases and service contracts to be made within governing board policies, source restrictions, funds availability, and other applicable 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 the review of independent supporting documentation for purchases and expenditures.

The Housing Authority executive director stated that the Housing Authority operated under the procurement guidelines within the property management agreement and the residential listing agreement, but had not considered such detailed purchasing oversight procedures.

The absence of adequate oversight for third-party vendor transactions increases the risk of errors or irregularities going undetected and possible misappropriation of funds.
Recommendation 32

We recommend that the Housing Authority develop and implement written procedures for oversight of purchasing activities by the property management firm and other third-party service vendors. Such oversight should require the submission of supporting vendor invoices and performance of a documented review/reconciliation.

Campus Response

We concur. The Housing Authority now requires the property management company and third-party service vendors to submit vendor invoices on a monthly basis and performs a documented review and reconciliation of these invoices. Formal written oversight procedures will be developed by October 31, 2009.
# APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CAMPUS</strong></td>
<td></td>
</tr>
<tr>
<td>Milton A. Gordon</td>
<td>President</td>
</tr>
<tr>
<td>Bill Barrett</td>
<td>Associate Vice President, Administration</td>
</tr>
<tr>
<td>Karen Bushman</td>
<td>Director, University Advancement Information Services</td>
</tr>
<tr>
<td>Paul Carey</td>
<td>Associate Vice President, University Advancement</td>
</tr>
<tr>
<td>Pat Carroll</td>
<td>Executive Assistant to the President</td>
</tr>
<tr>
<td>Amir Dabirian</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Naomi Goodwin</td>
<td>Assistant Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Willie Hagan</td>
<td>Vice President, Administration and Finance/Chief Financial Officer</td>
</tr>
<tr>
<td>Bahram Hatefi</td>
<td>Director, Internal Audit</td>
</tr>
<tr>
<td>Pamela Hillman</td>
<td>Vice President, University Advancement</td>
</tr>
<tr>
<td>Brian Jenkins</td>
<td>Associate Vice President, Finance</td>
</tr>
<tr>
<td>Chris Manrique</td>
<td>CMS Project Director</td>
</tr>
<tr>
<td>Robert Palmer</td>
<td>Vice President, Student Affairs</td>
</tr>
<tr>
<td>Steve Yim</td>
<td>Controller</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSU FULLERTON AUXILIARY SERVICES CORPORATION</strong></td>
<td></td>
</tr>
<tr>
<td>Fred Ambrozak</td>
<td>System Administrator</td>
</tr>
<tr>
<td>Allan Anaya</td>
<td>Manager, Nutwood Café</td>
</tr>
<tr>
<td>Kimberly Ball</td>
<td>Senior Manager, Text Department</td>
</tr>
<tr>
<td>Raul Castaneda</td>
<td>Senior Accountant</td>
</tr>
<tr>
<td>Shou-Yinn (Pearl) Cheng</td>
<td>Director, Sponsored Programs</td>
</tr>
<tr>
<td>Michael Clemons</td>
<td>Senior Manager, Titan Shops Operations</td>
</tr>
<tr>
<td>William Dickerson</td>
<td>Executive Director</td>
</tr>
<tr>
<td>Angie Dulay</td>
<td>Senior Manager, Titan Shops Tech Center</td>
</tr>
<tr>
<td>Cindy Fields</td>
<td>Payroll Specialist</td>
</tr>
<tr>
<td>Daniel Gaytan</td>
<td>Accountant</td>
</tr>
<tr>
<td>Ricky Glenn</td>
<td>Assistant Merchandise Manager</td>
</tr>
<tr>
<td>Judy Goberdhan</td>
<td>Accounts Payable Supervisor</td>
</tr>
<tr>
<td>Frank Herrera</td>
<td>Manager, Convenient Store</td>
</tr>
<tr>
<td>Omar Ifitikhar</td>
<td>Director, Management Information Systems</td>
</tr>
<tr>
<td>Tom Kinney</td>
<td>Receiving Manager</td>
</tr>
<tr>
<td>Chuck Kissel</td>
<td>Director, Titan Shops</td>
</tr>
<tr>
<td>Tony Lynch</td>
<td>Director, Food and Vending</td>
</tr>
<tr>
<td>Tariq Marji</td>
<td>Controller</td>
</tr>
<tr>
<td>Christina Martinez</td>
<td>General Manager, Food Court</td>
</tr>
<tr>
<td>Hanna Mengesha</td>
<td>Vault Manager</td>
</tr>
<tr>
<td>Lance Meredith</td>
<td>Senior System Administrator</td>
</tr>
<tr>
<td>Valerie Moreno</td>
<td>System Administrator/Food</td>
</tr>
<tr>
<td>Frank Mumford</td>
<td>Director, Finance and Administration</td>
</tr>
<tr>
<td>Ignacio Navarro</td>
<td>Manager, Concessions/Vending</td>
</tr>
<tr>
<td>Chi Nguyen</td>
<td>Grant Accountant</td>
</tr>
</tbody>
</table>
**APPENDIX A: PERSONNEL CONTACTED**

**CSU FULLERTON AUXILIARY SERVICES CORPORATION (CONT.)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sid Patel</td>
<td>Catering Manager</td>
</tr>
<tr>
<td>Valerie Ramirez</td>
<td>Manager, Carl’s Jr.</td>
</tr>
<tr>
<td>Maritza Rodriguez</td>
<td>Human Resource/Payroll Clerk</td>
</tr>
<tr>
<td>Smruti Shayan</td>
<td>Accounts Receivable Accountant</td>
</tr>
<tr>
<td>Kathryn Sowersby</td>
<td>Food Court Clerk</td>
</tr>
<tr>
<td>Sharlene Spicer</td>
<td>Receptionist</td>
</tr>
<tr>
<td>Mary Thoen</td>
<td>Coordinator, Sponsored Programs</td>
</tr>
<tr>
<td>Tanya Thompson</td>
<td>Assistant Director, Sponsored Programs</td>
</tr>
<tr>
<td>Stephen Weissbart</td>
<td>Data Entry Supervisor</td>
</tr>
</tbody>
</table>

**CSU FULLERTON PHILANTHROPIC FOUNDATION**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Karen Bushman</td>
<td>Director, Advancement Information Services</td>
</tr>
<tr>
<td>Paul Carey</td>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>Susan Cervantes</td>
<td>Accounting Services Coordinator</td>
</tr>
<tr>
<td>Julie Chung</td>
<td>Accounting Manager</td>
</tr>
<tr>
<td>Leo Garcia</td>
<td>Gift Processor</td>
</tr>
<tr>
<td>Pamela Hillman</td>
<td>Executive Director</td>
</tr>
<tr>
<td>Yvette Herrara</td>
<td>Administrative Assistant</td>
</tr>
<tr>
<td>Valerie Nguyen</td>
<td>Assistant Director, Advancement Information Services</td>
</tr>
</tbody>
</table>

**ASSOCIATED STUDENTS CALIFORNIA STATE UNIVERSITY, FULLERTON, INC.**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kurt Borsting</td>
<td>Director, Titan Student Union</td>
</tr>
<tr>
<td>Laura Brown</td>
<td>Director, Human Resources</td>
</tr>
<tr>
<td>Jeff Fehrn</td>
<td>Manager, Conference and Meeting Services</td>
</tr>
<tr>
<td>Betsy Gibbs</td>
<td>Director, Children’s Center</td>
</tr>
<tr>
<td>Ken Maxey</td>
<td>Manager, Titan Bowl and Billiards</td>
</tr>
<tr>
<td>Jeannie Mollenauer</td>
<td>Director, Financial Services</td>
</tr>
<tr>
<td>Ron Morris</td>
<td>Manager, Information Technology</td>
</tr>
<tr>
<td>Lydia Palacios</td>
<td>Office Coordinator, Children’s Center</td>
</tr>
<tr>
<td>Fred Sanchez</td>
<td>Executive Director</td>
</tr>
<tr>
<td>M. Pamela Skawin</td>
<td>Manager, Information Services</td>
</tr>
<tr>
<td>Steve Udell</td>
<td>Accounting Manager</td>
</tr>
<tr>
<td>Judith Valona</td>
<td>Executive Assistant</td>
</tr>
<tr>
<td>Andrea Willer</td>
<td>Director, Titan Recreation</td>
</tr>
</tbody>
</table>

**CSU FULLERTON HOUSING AUTHORITY**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>William Dickerson</td>
<td>Executive Director</td>
</tr>
<tr>
<td>Bill Herbert</td>
<td>Business Service Manager</td>
</tr>
<tr>
<td>Frank Mumford</td>
<td>Director, Finance and Administration</td>
</tr>
</tbody>
</table>
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.
DATE: September 14, 2009

TO: Larry Mandel
    University Auditor

FROM: Milton A. Gordon
    President

SUBJECT: Response for Auxiliary Organizations Audit Report 09-13

I am pleased to forward California State University, Fullerton’s official response to the thirty-two (32) recommendations in the Auxiliary Organizations Audit Report 09-13.

Once again, we would like to thank the University Auditor and his staff for conducting the audit in a professional manner and identifying meaningful ways to improve internal compliance and control in per the Board of Trustees Policy for The California State University Auxiliary Organizations.

The Campus Auditor, Bahram Hatefi, will also forward the responses to you electronically for your convenience. Should you have questions, please contact Bahram at 714-278-7299 or bhatefi@fullerton.edu.

Attachments

cc: Naomi Goodwin, Assistant Vice President, Administration & Finance
    Willie Hagan, Vice President, Administration & Finance CFO
    Bahram Hatefi, Director of CSUF Internal Audit
    Pamela Hillman, Vice President, University Advancement
    Chris Manriquez, Associate Vice President, Information Technology
    Robert Palmer, Vice President for Student Affairs
    Fred Sanchez, Executive Director ASI
AUXILIARY ORGANIZATIONS

CALIFORNIA STATE UNIVERSITY,
FULLERTON

Audit Report 09-13

CAMPUS

FISCAL COMPLIANCE

Recommendation 1

We recommend that the campus ensure that annual auxiliary cost allocation analyses are completed timely and formally approved, with signature and date, by the campus CFO or his designee.

Campus Response

We concur. All auxiliary cost allocation analyses identified above were signed and dated by the Associate Vice President of Finance during audit field work and remain current. Future annual auxiliary cost allocation analyses will be completed timely and formally approved, with signature and date, by the Associate Vice President of Finance.

INFORMATION TECHNOLOGY

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Recommendation 2

We recommend that the campus and auxiliaries:

a. Define and document roles and responsibilities for PCI compliance between the campus and auxiliaries.

b. Conduct a risk assessment of comprehensive compliance obligations for credit card data maintained on auxiliary servers and transmitted throughout the campus network.

c. Complete an annual SAQ to include all credit card merchants on campus, whether completed jointly or separate from the auxiliaries.

Campus Response

We concur.

a. The campus has developed a standard for the acceptance of credit cards which defines administrative, technical and user roles and responsibilities and establishes centralized processes for reviewing all organizational requests for accepting credit cards.
b. We concur. The Information Security Office annually conducts a Protected Data survey across all campus divisions. The developed University Standard for the Acceptance of Credit Cards specifically states "The Information Security Office will perform a yearly risk assessment of comprehensive compliance obligations for credit card data maintained on all campus and auxiliary servers which transmit data throughout the campus network. The assessment will be the principle tool used to complete the required PCI self-assessment". The 2009-2010 Protected Data survey will be completed by December 23, 2009.

c. We concur. ASC, ASI, Foundation and the campus have completed the 2008-2009 annual SAQ assessment and have either retained this assessment for the record or have forwarded the assessment to the respective acquirer, as specified by the acquirer.

**USER ACCESS REVIEWS**

**Recommendation 3**

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

**Campus Response**

We concur.

We concur. ASC and the Housing Authority will conduct annual documented management reviews of user access for all systems containing protected data. The review for year 2009-10 will be completed by September 30th, 2009.

ASI has implemented a policy to perform periodic documented management reviews of user access privileges within the critical systems and those systems containing protected data. This review was performed in September 2009 and will be performed on an annual basis.

We concur. CSFPF will conduct annual documented management reviews of user access for all systems containing protected data by June 30th of each year. The review for year 2009-10 was completed on June 30, 2009.

**INFORMATION SECURITY TRAINING**

**Recommendation 4**

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

**Campus Response**

We concur. The auxiliaries will develop and implement an action plan by November 5, 2009.
OPERATING AND ADMINISTRATIVE AGREEMENTS

Recommendation 5

We recommend that the Corporation:

a. Promptly renew the agreements with the noted service providers.

b. Implement a process to ensure that all future agreements are timely renewed and include an appropriate indemnification provision.

Campus Response

We concur. The Corporation has renewed the agreements with the noted service providers and implemented a process to ensure that all future agreements are timely renewed and include an appropriate indemnification provision.

CORPORATE GOVERNANCE

Recommendation 6

We recommend that the Corporation ensure that appropriate board representation is maintained.

Campus Response

We concur. The Corporation will ensure appropriate board representation is maintained by October 31, 2009.

OPERATIONAL COMPLIANCE

Recommendation 7

We recommend that the Corporation develop and implement written procedures to address the transfer of inventory from the bookstore centralized receiving dock to satellite locations. Such procedures should include documentation of inventory quantity and type transferred, handling of inventory transferred, safeguards over inventory in transit, and acknowledgement of receipt of inventory transferred.

Campus Response

We concur. The Corporation will develop procedures to address the transfer of inventory from the bookstore centralized receiving dock to satellite locations, including documentation of inventory quality and type, inventory transfer handling, safeguards during transit, and acknowledgement of receipt, by October 31, 2009.
PROGRAM COMPLIANCE

Recommendation 8

We recommend that the Corporation establish and implement a process to report all student intern stipends to the campus financial aid office.

Campus Response

We concur. The Corporation will develop and implement a process to report all student intern stipends to the campus financial aid office by October 31, 2009.

CASH RECEIPTS AND HANDLING

Recommendation 9

We recommend that the Corporation develop written policies and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery.

Campus Response

We concur. The Corporation will develop written policies and procedures to address cash shortages and/or overages, including mitigation, investigation, and recovery by October 31, 2009.

TRUSTS AND OTHER LIABILITIES

Recommendation 10

We recommend that the Corporation:

a. Complete a review of all custodial trust accounts reflected as “deposits held for others” on its financial statements and determine, within 60 days, which accounts contain state funds.

b. Submit to the Office of the University Auditor, within 60 days, a list of those custodial trust accounts which have been deemed appropriate to remain in the custody of the Corporation and comprehensive documentation to support the sources of funds for those trust accounts.

c. Move those state funds identified in “a” above to campus accounts within six months.

Campus Response

We concur. The campus will complete a review of all custodial trust accounts and submit to the Office of the University Auditor by November 10, 2009 a list of those accounts deemed appropriate to remain in the custody of the Corporation and comprehensive documentation to support the sources of funds for those trust accounts. Any state funds identified will be moved to campus accounts within six months.
AUXILIARY PROGRAMS

Recommendation 11

We recommend that the Corporation reiterate to staff cost share and effort certification requirements and implement a process to ensure the completion of cost share and effort certification reports.

Campus Response

We concur. The Corporation will reiterate to staff cost share and effort certification requirements and will work with the university to implement a process to ensure the completion of cost share and effort certification reports by October 31, 2009.

INFORMATION TECHNOLOGY

PASSWORD SECURITY

Recommendation 12

We recommend that the Corporation:

a. Implement a shadow password file for the IFAS.

b. Set effective password security parameters for the MBS and IFAS in accordance with campus guidelines and perform an assessment of password security parameters for all other Corporation systems.

Campus Response

We concur. The IFAS server is now running in HP-UX Trusted Mode, allowing the system to run at C-2 level security, store passwords in an encrypted database, and assign a minimum password length of 8. Password security parameters have been established in accordance with campus guidelines for MBS, IFAS, and all other Corporation systems.

PROTECTED DATA ASSESSMENT AND SECURITY

Recommendation 13

We recommend that the Corporation:

a. Properly secure all systems and servers containing critical and protected data.

b. Encrypt the storage and transfer of payroll files contained within the “payroll records super directory.”

c. Perform an assessment and inventory of protected data on all Corporation servers, including administrative file servers, to determine the existence of any protected data and the need for appropriate logical and physical security measures.
Campus Response

We concur. All systems and servers containing protected data are now located in the computer center behind a NetScreen firewall administered by the university’s IT division and stored and transferred payroll records files are now encrypted. An inventory and assessment of protected data on Corporation servers to determine the need for additional security measures is in progress and will be completed by October 31, 2009.

DATA CONFIDENTIALITY FORMS

Recommendation 14

We recommend that the Corporation:

a. Establish a policy requiring data confidentiality forms from all employees prior to granting them access to critical systems and protected data.

b. Obtain completed forms from personnel who currently have access to such data.

Campus Response

We concur. The Corporation has adopted the University’s policy requiring confidentiality forms from all employees prior to granting access protected data. Obtaining completed forms from personnel who currently have access to such data was completed in conjunction with the system-wide information security training initiated in March 2009.

SYSTEM BACKUPS

Recommendation 15

We recommend that the Corporation:

a. Encrypt system backups with protected data.

b. Strengthen procedures to ensure that the transfer to, and storage of, backups at the bookstore are adequately controlled.

C. Evaluate the security benefits of contracting with an off-campus backup storage facility, including the opportunity to merge backup processes with the campus.

Campus Response

We concur. The Corporation will work with university to evaluate mechanisms of encrypting backups with protected data by December 31, 2009 and has already contracted with an off-campus back up storage facility to ensure back-up transfer and storage is adequately controlled.
REMOTE SERVER ACCESS

Recommendation 16

We recommend that the Corporation 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 VPN connection has been established.

Campus Response

We concur. The Corporation will work with university to enforce internal firewall restrictions on Telnet such that it can only be accessed once a VPN connection has been established by December 31, 2009 or replace Telnet remote access with a more secure remote access protocol (such as secure shell).

DISASTER RECOVERY PLAN

Recommendation 17

We recommend that the Corporation complete a written information technology disaster recovery plan.

Campus Response

We concur. A written information technology disaster recovery plan is now complete and will be officially adopted by the Corporation by October 31, 2009.

ENVIRONMENTAL CONTROLS

Recommendation 18

We recommend that the Corporation evaluate the feasibility of another means of fire suppression other than water sprinklers or implement mitigating controls to ensure that all servers are not damaged from any resulting flooding.

Campus Response

We concur. The Corporation will work with the building property manager to evaluate the feasibility for another means of fire suppression other than water or implement to ensure all servers are protected from potential fire system water damage by November 30, 2009.
CSU FULLERTON PHILANTHROPIC FOUNDATION

FISCAL COMPLIANCE

Recommendation 19

We recommend that the Foundation develop a written reserve policy to address the allocation of surplus funds/reserves. Such a policy should address minimum reserve requirements, board review of reserve levels, reserves for working capital and capital replacement, and the methodology used for the calculation of reserves.

Campus Response

We concur. A reserve policy was adopted by the CSFPF Board of Governors on May 1, 2009. The policy among other things addresses the allocation of surplus funds/reserves.

OPERATIONAL COMPLIANCE

Recommendation 20

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

Campus Response

We concur. The CSFPF is preparing a draft risk management policies. The draft policy will be presented to the Board of Governors for adoption by February 26, 2010.

FEES, REVENUES, AND RECEIVABLES

Recommendation 21

We recommend that the Foundation ensure that donor credit card information is stored in compliance with PCI standards and that safeguards be implemented to ensure that protected data is adequately secured.

Campus Response

We concur. The CSFPF, in coordination with the Office of University Advancement, redacts written credit card information. Credit card information is no longer stored on the FileNet system. The SmartCall telemarketing system uses encrypted technology.
ENDOWMENT ADMINISTRATION

Recommendation 22

We recommend that the Foundation:

a. Implement a process to ensure the establishment and execution of endowment agreements.

b. Revise its endowment agreement to specifically address the Foundation’s management fees and annual spending policy.

Campus Response

We concur.

a. The CSFPF will advise all directors of development and UA fundraising personnel of the requirement for review of draft endowment agreements by the CSFPF CFO prior to the submission to potential donors. Endowment agreements are not fully executed until approved and signed by the Vice President for University Advancement and the CSFPF CFO.

b. The CSFPF has revised its endowment agreement to include explanations of the endowment management fee and the annual spending policy.

INFORMATION TECHNOLOGY

Recommendation 23

We recommend that the Foundation reassess its security requirements and set effective password security controls for its computer systems.

Campus Response

We concur. The CSFPF information technology security requirements will be reassessed in coordination with the scheduled upgrade to an Oracle platform. The CSFPF will also reassess password security controls after Oracle implementation is completed on December 31, 2009.
ASSOCIATED STUDENTS  
CALIFORNIA STATE UNIVERSITY, FULLERTON, INC.  

FISCAL COMPLIANCE  

Recommendation 24  

We recommend that AS account for and track UBI for Titan Bowl and Billiards services provided to community members, and file federal income tax returns as appropriate.  

Campus Response  

ASI will engage our external auditor to thoroughly review all operations and types of revenue for an official opinion on revenue types to be reported as unrelated business activity. ASI will comply with the independent auditor’s recommendation for future tax reporting. We anticipate that we will have a response from our external auditor by October 2009 and will proceed accordingly.  

CASH RECEIPTS AND HANDLING  

Recommendation 25  

We recommend that AS:  

a. Implement the use of transfer receipts when funds are transferred between locations.  

b. Establish a written policy for the transport of deposits between locations and increase cashiers’ awareness of the availability of security escorts when deposits are transferred from outlying areas and in the event of large deposits.  

Campus Response  

We concur.  

a. A transfer receipt will be utilized when funds are transferred between locations. We are in the process of implementing a standard transfer receipt/transfer log to be used by all departments. This will be completed by November 2009.  

b. We have implemented a policy to specify that when $3,000 or more in cash (currency and coin) is being transported from the central cash vault to any ASI department, or from any ASI department to the central cash vault, cash will be transported by two people or by utilizing the services of a public safety escort. A “Cash Transport Policy” was drafted and implemented in April 2009.
FEES, REVENUES, AND RECEIVABLES

Recommendation 26

We recommend that AS:

a. Formally document collection activity of delinquent accounts receivable in order to facilitate collection or to support write-off.

b. Establish and implement written policies and procedures for the monitoring of accounts receivable, the collection of delinquent agency accounts and third-party receivables, and bad debt write-offs.

Campus Response

We concur. ASI has implemented policies and procedures addressing the process and documentation of collection activity and/or write-off of past-due accounts. A “Collection of Past Due Accounts” policy was drafted and implemented in June 2009.

PURCHASING AND ACCOUNTS PAYABLE

Recommendation 27

We recommend that AS:

a. Enforce accounts payable procedures to ensure that agency accounts and athletic department disbursements are processed in accordance with AS accounts payable procedures.

b. Reiterate to staff existing cash disbursement policies and procedures regarding sufficient and appropriate supporting documentation and authorization.

Campus Response

We concur.

a. We will process ASI disbursements in compliance with our accounts payable procedures and will revise ASI policies and procedures to clarify our practice with regard to funds held for others, specifically Agency and Athletics accounts. We revised our “Agency Accounts” policy effective August 2009. We also implemented an “Athletics Accounting” policy effective August 2009. We will revise our accounting services agreement with Athletics to reflect these policies by November 2009.

b. ASI has cash disbursement policies and procedures in place that outline appropriate supporting documentation and authorization. These were distributed in June 2009 to every department and program ASI funds as part of the annual budget process for fiscal year 2009-2010. As a follow-up, we will send out notice each semester reminding staff of the need for strict compliance with these budget policies and procedures.
INFORMATION TECHNOLOGY

PASSWORD SECURITY

Recommendation 28

We recommend that AS:

a. Reassess its security requirements and set effective password security controls for Counterpoint and IFAS systems in accordance with campus guidelines and perform an assessment of password security parameters for all other AS systems.

b. Clarify and document the security responsibilities of systems administrators, specifically for password and login security parameters.

Campus Response

We concur. The Application Administrators have been trained to review and change the password and login security parameters for all critical systems with protected data. This training took place in July 2009. The IT Systems Administrator will periodically review login security parameters for all critical systems with protected data. This was accomplished in August 2009 and will be reviewed annually. With regard to password character lengths, we will now enforce the use of 8-character password lengths for all systems (effective July 2009).

ENVIRONMENTAL CONTROLS

Recommendation 29

We recommend that AS implement a fire and smoke detection system in the server room.

Campus Response

We concur. We have installed a smoke detector in the ASI data center.
CSU FULLERTON HOUSING AUTHORITY

CORPORATE GOVERNANCE

Recommendation 30

We recommend that the Housing Authority promptly file the cited amendments with the chancellor’s office and develop a procedure to ensure that all future changes/amendments to Articles of Incorporation are timely filed with the chancellor’s office.

Campus Response

We concur. The cited amendments were resubmitted to the Chancellor’s Office in March, 2009, and a procedure to ensure that all future amendments to Articles of Incorporation are submitted timely and a record of these submissions is maintained in Housing Authority files.

SEGREGATION OF DUTIES

Recommendation 31

We recommend that the Housing Authority appropriately segregate certain cash receipts processing functions or institute mitigating procedures approved by the campus CFO.

Campus Response

We concur. Cash receipts processing has been appropriately segregated.

PURCHASING AND ACCOUNTS PAYABLE

Recommendation 32

We recommend that the Housing Authority develop and implement written procedures for oversight of purchasing activities by the property management firm and other third-party service vendors. Such oversight should require the submission of supporting vendor invoices and performance of a documented review/reconciliation.

Campus Response

We concur. The Housing Authority now requires the property management company and third-party service vendors to submit vendor invoices on a monthly basis and performs a documented review and reconciliation of these invoices. Formal written oversight procedures will be developed by October 31, 2009.
October 7, 2009

MEMORANDUM

TO: Mr. Larry Mandel  
University Auditor

FROM: Charles B. Reed  
Chancellor

SUBJECT: Draft Final Report 09-13 on *Auxiliary Organizations*,  
California State University, Fullerton

In response to your memorandum of October 7, 2009, I accept the response as submitted with the draft final report on *Auxiliary Organizations*, California State University, Fullerton.

CBR/amd