

**AUXILIARY ORGANIZATIONS**  
**CALIFORNIA STATE UNIVERSITY,**  
**MONTEREY BAY**

**Audit Report 08-53**  
**May 14, 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 Auditor: Ken Tsui  
Internal Auditor: Jamarr Johnson

---

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

---

## CONTENTS

Executive Summary .....	1
Introduction .....	4
Background .....	4
Purpose .....	5
Scope and Methodology .....	5

---

## OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

### **CAMPUS**

Fees, Revenues, and Receivables .....	8
Purchasing and Accounts Payable .....	9

### **UNIVERSITY CORPORATION AT MONTEREY BAY**

Operating and Administrative Agreements .....	11
Corporate Governance .....	12
Operational Compliance .....	13
Segregation of Duties .....	14
Fees, Revenues, and Receivables .....	15
Auxiliary Programs .....	15
Information Technology .....	17
Password Security .....	17
User Access Reviews .....	18
Protected Data Assessment and Security .....	19
Payment Card Industry Data Security Standard .....	21
Information Security Training .....	22
System Backups .....	23

### **CSUMB EMPLOYEE HOUSING, INC.**

Corporate Governance .....	25
----------------------------	----

## **APPENDICES**

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

---

## **ABBREVIATIONS**

CEHI	CSUMB Employee Housing, Inc.
CIO	Chief Information Officer
Corporation	University Corporation at Monterey Bay
CSU	California State University
CSUMB	California State University, Monterey Bay
DMZ	Demilitarized Zone
EO	Executive Order
KAZU	KAZU Radio Station
OMB	Office of Management and Budget
PCI DSS	Payment Card Industry Data Security Standards
RFIN	Resolution of the Committee on Finance
SAQ	Self-Assessment Questionnaire

---

## 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, Monterey Bay (CSUMB) 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 CSUMB campus and its auxiliary organizations from December 1, 2008, through December 17, 2008, and made a study and evaluation of the system of internal compliance/internal control in effect as of December 17, 2008. This report represents our triennial review.

Our study and evaluation at the *University Corporation at Monterey Bay* revealed certain conditions that, in our opinion, could result in errors and irregularities if not corrected. Specifically, the auxiliary did not maintain adequate control over information technology. These conditions, along with other reportable weaknesses, are described in the executive summary and in the body of the report. In our opinion, except for the weakness described above, accounting and administrative control in effect as of December 17, 2008, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at the *CSUMB Employee Housing, 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 other reportable weaknesses that are described in the executive summary and in the body of the report. In our opinion, the accounting and administrative

control in effect as of December 17, 2008, 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**

#### **FEES, REVENUES, AND RECEIVABLES [8]**

The campus did not document the processing of matching gifts and review of donor terms prior to the deposit of matching gift funds.

#### **PURCHASING AND ACCOUNTS PAYABLE [9]**

Campus oversight of purchasing activities performed by a third-party property management firm for the University Corporation at Monterey Bay student housing and the CSUMB Employee Housing, Inc. employee housing was not adequate.

### **UNIVERSITY CORPORATION AT MONTEREY BAY**

#### **OPERATING AND ADMINISTRATIVE AGREEMENTS [11]**

Certain agreements among the University Corporation at Monterey Bay, the California State University (CSU) Trustees, and the campus did not include appropriate indemnification clauses. This is a repeat finding from the prior auxiliary organizations audit for the operating agreement between the Corporation and the CSU Trustees.

#### **CORPORATE GOVERNANCE [12]**

The Corporation had not filed amended Articles of Incorporation with the chancellor's office in a timely manner.

### **OPERATIONAL COMPLIANCE [13]**

The Corporation did not ensure that the KAZU Radio Station (KAZU) developed policies and procedures to address the accounting and processing of cash receipts/handling and accounts receivable.

### **SEGREGATION OF DUTIES [14]**

Duties and responsibilities over certain payroll functions were not properly segregated at the Corporation. This is a repeat finding from the prior auxiliary organizations audit.

### **FEES, REVENUES, AND RECEIVABLES [15]**

Forms containing credit card information from KAZU donors were not stored in a locked cabinet with controlled access.

### **AUXILIARY PROGRAMS [15]**

Sub-recipient monitoring was not always adequate, and formal policies and procedures for sub-recipient monitoring of contracts and grants were inadequate at the Corporation.

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

Password security parameters were not always adequate for Corporation systems, and the Corporation did not perform a periodic documented management review of user access privileges within all systems and applications containing protected data. The Corporation did not perform a periodic assessment and inventory of protected information residing on its systems, and internal resources were not adequately protected. Further, the Corporation had not completed a Payment Card Industry (PCI) Data Security Standard (DSS) Self-Assessment Questionnaire or any other PCI DSS compliance summary plan to define their applicable vendor level and respective contractual requirements. In addition, Corporation, KAZU, and university advancement personnel with access to sensitive donor and financial information were not always required to complete information security awareness training; and daily, weekly, and monthly backups for Corporation systems with protected data were not encrypted when stored locally or when in transit to the off-site storage location.

### **CSUMB EMPLOYEE HOUSING, INC.**

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

CSUMB Employee Housing, Inc. had not filed amended Articles of Incorporation with the chancellor's office in a timely manner.

---

## INTRODUCTION

### **BACKGROUND**

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

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

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

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

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

The University Corporation at Monterey Bay (Corporation) is the entity responsible for the post-award administration of sponsored programs, student housing, conference services, the Otter Student Union, and the KAZU radio station. The Corporation oversees a number of other commercial operations and outsources management/operating services. The bookstore is operated by Barnes and Noble, and campus dining and the child development center are managed by Sodexo and Children's Services, Inc., respectively. The Corporation, in cooperation with campus administrative offices, provides fiscal administrative and support services for grants and contracts for research, instruction, and public service;

---

## INTRODUCTION

instructionally related programs, conferences, workshops, and institutes; private gifts and other support sources to the university; and agency activities as requested by the university.

The CSUMB Employee Housing, Inc. (CEHI) 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. CEHI is a single-purpose auxiliary with no dedicated employees; property management services have been outsourced to Alliance Property Management, and all administrative and accounting services are provided by the Corporation. CEHI oversees the rental program, and the construction, financing, sales, and resales of the for-sale program, plus community/property management. CEHI is independently managed and governance is provided by a nine-member board of directors comprised of faculty, staff, student, homeowner, and community representatives. CEHI is anticipated to be reviewed for dissolution into the Corporation in the first quarter of 2009.

### **PURPOSE**

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

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

### **SCOPE AND METHODOLOGY**

Our study and evaluation were conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors, and included the audit tests we considered necessary in determining that accounting and administrative controls are in place and operative. The management review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor policies, letters, and directives. For those audit tests that required annualized data, fiscal years 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 December 17, 2008. 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:

University Corporation at Monterey Bay

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

CSUMB Employee Housing, Inc.

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

Campus

- ▶ Campus Oversight and Control

We have not performed any auditing procedures beyond December 17, 2008. 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

#### FEES, REVENUES, AND RECEIVABLES

The administration of corporate matching gifts required improvement.

We found that the campus did not utilize a matching gifts form or other method to document matching gift processing and an eligibility review of corporate donor terms prior to the deposit of matching funds to a specifically directed recipient.

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

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

The advancement services manager stated that these best practice guidelines for matching gifts had not been considered due to the small volume of matching gift transactions.

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

#### **Recommendation 1**

We recommend that the campus develop a matching gifts form or other method to document matching gift processing and the review of donor terms prior to the deposit of matching funds to a specifically directed recipient.

#### **Campus Response**

We concur. The Corporation will develop a matching gifts form or other method to document matching gift processing and the review of donor terms prior to the deposit of such gifts. This will be completed by August 31, 2009.

## **PURCHASING AND ACCOUNTS PAYABLE**

Campus oversight of purchasing activities performed by a third-party property management firm for the University Corporation at Monterey Bay (Corporation) student housing and CSUMB Employee Housing, Inc. (CEHI) employee housing was not adequate.

The written agreement with the property management firm required that it establish an annual budget for operating expenses associated with student and employee housing. During the year, the property management firm had access to housing funds and was allowed to procure goods and services for both housing operations. The Corporation and CEHI subsequently reviewed these transactions based on accounting data submitted by the property management firm and then input the data into the Corporation 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.

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 Corporation accounting manager stated that the Corporation and CEHI were operating under the procurement guidelines within the property management 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 2**

We recommend that the campus work in conjunction with the Corporation and CEHI to develop and implement procedures for oversight of purchasing activities. Such oversight should require the property management firm to submit supporting vendor invoices and Corporation and CEHI management to perform a documented review/reconciliation.

**Campus Response**

We concur. The Corporation and CEHI will work in conjunction with the campus to develop and implement procedures for oversight of purchasing activities performed by the third-party property management firms. These procedures will include a documented review/reconciliation of supporting vendor invoices provided by the third-party property management firm. The procedures will be implemented by October 31, 2009.

## **UNIVERSITY CORPORATION AT MONTEREY BAY**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS**

Certain agreements among the University Corporation at Monterey Bay (Corporation), the CSU Trustees, and the campus did not include appropriate indemnification clauses.

We found that:

- ▶ The indemnification clause in the operating agreement between the Corporation and the CSU Trustees did not specifically indemnify the campus. This is a repeat finding from the prior auxiliary organizations audit.
- ▶ The indemnification and save harmless clause in the administrative services agreement between the Corporation and the campus did not specifically indemnify the State of California and the CSU Trustees.

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

The Corporation director of operations stated that a revised operating agreement had not been executed since the last audit due to oversight. She further stated that she was unaware that this clause was necessary for service agreements.

The absence of appropriate indemnification clauses subjects the campus and CSU to potential liability.

#### **Recommendation 3**

We recommend that the Corporation amend the cited agreements to include appropriate indemnification clauses and ensure that future agreements include appropriate indemnification clauses.

#### **Campus Response**

We concur. The cited agreements will be amended to include the appropriate indemnification clauses. This will be completed by August 31, 2009. Future agreements will include appropriate indemnification clauses.

## CORPORATE GOVERNANCE

The Corporation had not filed amended Articles of Incorporation with the chancellor's office in a timely manner.

We found an amendment to the Articles of Incorporation made on June 26, 2008, that had not been filed with the chancellor's office until noted during our review.

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 Corporation director of operations stated that the amended Articles of Incorporation were not submitted timely to the chancellor's office due to oversight. She further stated that the amended Articles of Incorporation were submitted to Financing and Treasury at the chancellor's office via email on December 22, 2008.

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

### **Recommendation 4**

We recommend that the Corporation 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 amended Articles of Incorporation were submitted to Financing and Treasury at the chancellor's office via email on December 22, 2008. This task has been added to the administrative assistant's procedure manual as a board meeting follow-up task. This recommendation was implemented in May 2009.

## OPERATIONAL COMPLIANCE

The Corporation did not ensure that the KAZU Radio Station (KAZU) developed policies and procedures to address the accounting and processing of cash receipts/handling and accounts receivable.

Specifically, procedures should address:

- ▶ Handling, safeguarding, depositing, and recording of donor and sponsor payments.
- ▶ Sufficient documentation of receipts and donor information.
- ▶ Billing and recording of amounts due.
- ▶ Aging and collection of pledges receivable.
- ▶ Write-off of uncollectible pledges receivable.

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

The KAZU general manager stated that KAZU generally adhered to the Corporation's accounting policies and procedures. He further stated that policies and procedures specifically applicable to KAZU's accounting process had not been developed due to oversight.

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

### **Recommendation 5**

We recommend that the Corporation ensure that KAZU develop written policies and procedures to address the accounting and processing of cash receipts/handling and accounts receivable.

### **Campus Response**

We concur. The Corporation will develop written procedures for KAZU to address the accounting and processing of cash receipts/handling and accounts receivable. The procedures will be implemented by October 31, 2009.

## SEGREGATION OF DUTIES

Duties and responsibilities over certain payroll functions were not properly segregated at the Corporation. This is a repeat finding from the prior auxiliary organizations audit.

We found that one employee:

- ▶ Entered the number of hours worked.
- ▶ Processed the payroll information.
- ▶ Received the payroll checks prior to disbursement of those checks.

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

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.6, *Payroll*, states that the auxiliary should establish a written control system that ensures payroll preparation is segregated from the general ledger function and other payroll functions such as hiring authorization, timekeeping, and distribution of checks.

The Corporation director of operations stated that staffing constraints and workload issues led to the lack of proper oversight and appropriate segregation of duties at the Corporation.

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

### **Recommendation 6**

We recommend that the Corporation ensure that payroll functions are properly segregated or institute mitigating procedures approved by the campus chief financial officer.

### **Campus Response**

We concur. The Corporation has properly segregated payroll functions. The HR/Accounting administrative assistant receives timesheets and verifies hours. Then, the payroll technician enters hours worked as part of the payroll process. The Corporation controller or her designee verifies payroll. Human resources staff receives the checks prior to disbursement. This recommendation was implemented in May 2009.

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

Forms containing credit card information from KAZU donors were not stored in a locked cabinet with controlled access.

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 KAZU general manager stated that donation forms containing credit card information were not properly safeguarded due to oversight.

Insufficient control over access to sensitive donor information increases the risk of unauthorized and inappropriate acts.

### **Recommendation 7**

We recommend that the Corporation ensure that KAZU properly safeguards forms containing donor credit card information.

### **Campus Response**

We concur. KAZU now properly safeguards forms containing donor credit card information by requiring this information to be in the possession of a KAZU employee at all times and to be locked in a cabinet in a locked office overnight. This recommendation was implemented in May 2009.

## **AUXILIARY PROGRAMS**

Sub-recipient monitoring was not always adequate, and formal policies and procedures for sub-recipient monitoring of contracts and grants were inadequate at the Corporation.

Our review of ten contracts and grants files and corresponding sub-awards disclosed that A-133 reports had not been received and reviewed for two sub-recipients. In addition, it was noted that the Corporation lacked adequate policies for the request and review of sub-recipient A-133 audit reports and audited financial statements prior to the award of sub-awards, and for the monitoring of resolution of any instances of non-compliance with federal regulations addressed within the audit reports.

The Corporation *Policy 511-004-A: Sub-award Administration for External Funding* states that the project director/principal investigator also has primary responsibility for the monitoring of sub-recipients to ensure compliance with federal regulations and with the terms and conditions of both the primary award and sub-award. Resolution of complex sub-recipient monitoring issues or the determination of courses of action will be done jointly by the project director/principal investigator, grants and contracts office, Corporation grants accounting, purchasing and/or other appropriate administrative officials.

Office of Management and Budget (OMB) Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, §320, states that auditees that are also sub-recipients shall submit to each pass-through entity one copy of the reporting package described in paragraph (c) of this section for each pass-through entity when the schedule of findings and questioned costs disclosed audit findings relating to federal awards that the pass-through entity provided or the summary schedule of prior audit findings reported the status of any audit findings relating to federal awards that the pass-through entity provided.

OMB Circular A-110, *Uniform Administrative Requirements for Grants and Agreements With Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations*, §.51(a), states that recipients are responsible for managing and monitoring each project, program, sub-award, function, or activity supported by the award. It also states that, "recipients shall monitor sub-awards to ensure sub-recipients have met the audit requirements," defined in OMB Circular A-133.

The Corporation controller stated that one of these grants did not have sub-award expenditures at the time that sub-recipient letters were sent in June. She added that the other grant sub-recipient was sent request letters in June and July, but no response had been received.

Failure to monitor sub-recipient activities increases the risk of non-compliance with federal regulations and jeopardizes the future of the Corporation's grant programs.

### **Recommendation 8**

We recommend that the Corporation:

- a. Complete a proper review of the two sub-recipients that had not provided A-133 reports.
- b. Strengthen its policies and procedures to ensure the timely request, receipt, review of A-133 audit reports, and resolution of applicable findings prior to the granting of federally funded sub-awards to the sub-recipients.

### **Campus Response**

We concur.

- a. The Corporation will complete a proper review of the two sub-recipients that had not provided A-133 reports. This will be completed by September 30, 2009.

- b. The grants and contracts office now requires the receipt and review of A-133 audit reports and resolution of applicable findings prior to the granting of federally funded sub-awards to sub-recipients. In the absence of an A-133 report, an annual financial statement will be requested. This recommendation was implemented in May 2009.

## INFORMATION TECHNOLOGY

### PASSWORD SECURITY

Password security parameters were not always adequate for Corporation systems.

The following password security parameters were set outside of leading security standards:

#### Active Directory:

- ▶ Minimum Password Length = At least four characters.
- ▶ Maximum Password Age = 500 days.
- ▶ Minimum Password Age = Allow changes immediately.

#### Raiser's Edge Donor System:

- ▶ Passwords never expire.
- ▶ No minimum password length.
- ▶ No password complexity requirements.
- ▶ No account lock-out settings (for login failures).

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

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

The campus director of network services stated that the Active Directory password parameters were inadequate due to oversight. The campus associate director of information systems stated that the Raiser's Edge system did not allow changes to the vendor-established password controls.

Insufficient password and login parameters and account lock-out settings 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 9**

We recommend that the Corporation reassess its security requirements and set effective password security controls and account lock-out settings for its computer systems.

### **Campus Response**

We concur. Whenever possible, the university will implement strong password security based on the CSU System-wide Information Security Standards. Based on these guidelines, the following controls will be implemented:

- PeopleSoft – Completed verification of password history depth setting.
- Active Directory – (<http://it.csUMB.edu/news.php?id=5305>) Implemented June 1, 2009.
- Raiser's Edge – (<http://forums.blackbaud.com/blogs/raisersedge/archive/2009/03/30/exciting-password-changes-on-the-horizon.aspx>) Will be completed by August 31, 2009.

### **USER ACCESS REVIEWS**

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

We found that while annual user access reviews were documented for the financial and human resources modules of PeopleSoft, annual user access reviews were not documented for the ADP payroll system or the Raiser's Edge donor system.

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

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 Corporation controller stated that while management's review of other auxiliary systems had been documented, the Corporation had not considered the need to document reviews of user access within the donor and payroll systems.

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

### **Recommendation 10**

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

### **Campus Response**

We concur. Information technology in collaboration with the Corporation will review and develop guidelines for information security access, to include but not be limited to, approval of data access requests and management review of user access privileges. The guidelines will be implemented by November 30, 2009.

## **PROTECTED DATA ASSESSMENT AND SECURITY**

The Corporation did not perform a periodic assessment and inventory of protected information residing on its systems, and internal resources were not adequately protected.

We found that:

- ▶ The Corporation had not conducted a detailed assessment of protected information residing on auxiliary systems, and the protected information was not formally inventoried.
- ▶ The ADP payroll system with protected employee data was not encrypted.
- ▶ Departmental shared drives on Corporation file servers were not encrypted and an assessment of protected data had not been conducted so the existence of protected data was unknown.
- ▶ The lack of a demilitarized zone (DMZ) increased the risk of internal network exposure to security compromises as all file, application, and database servers were located within 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 periodic assessment and inventory of protected information residing on auxiliary systems, as well as the protection and encryption of any protected data residing on systems.

The campus interim chief information officer (CIO) stated that the protected data assessment and inventory of auxiliary systems had not been conducted as a result of competing information

technology priorities and significant management turnover. The campus associate director of information systems stated that the ADP system was not encrypted due to limitations in the ADP vendor software. The campus director of network services stated that a DMZ was not in place between web servers and internal campus resources due to insufficient resources to fund such a project.

Inadequate accountability over information assets, especially those containing 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 11**

We recommend that the Corporation:

- a. Conduct an assessment and inventory of protected information, and ensure that a reassessment is completed, at least annually. Such an assessment would reference applications, servers/systems, databases, storage locations, protected data types, approximations for number of protected data files, existing security controls, interfaces with other systems, custodians of record, technical security officers, and individuals permitted access.
- b. Properly secure all systems and servers containing protected data.
- c. Evaluate the feasibility of implementing a DMZ to separate and protect internal campus resources from Internet-accessible devices.

### **Campus Response**

We concur.

- a. Information technology in collaboration with the Corporation will work to define, assess, and secure protected data residing in auxiliary systems and university file servers. This assessment will be conducted on an annual basis. A review of the ADP payroll system will be completed by August 31, 2009, and all attempts will be made to ensure the application complies with the security policy.
- b. A review of physical and virtual security is underway by Network Services at this time. Currently, all university-owned systems are physically secured in an access-restricted facility in building 41A. Virtual security is addressed below.
- c. At this time, most campus servers are protected by software firewalls that filter sensitive TCP/UDP ports from campus and external access. The current edge dual Juniper ISG 2000 firewalls filter traffic to internal campus servers based on source, destination, and TCP/UDP ports. Traffic originating from the residential network (including dormitories and the cable modem system) is physically separated from the campus using firewalls so that every transaction is filtered through the edge firewalls as well. At this time, the Network Services group is

developing a server security DMZ implementation plan. This plan will include separate DMZ zones for database, applications, and web front-end applications. Servers will be placed in their own specific IP subnets by function, and their traffic will transverse the firewall from one zone to the other. The plan is part of the ITRP2 project that will provide two Juniper ISG2000 firewalls that will be used for the DMZ zones and control internal and external user access to servers and intra-zone server communications. Network Services has completed the necessary design and implementation plans and is awaiting chancellor's office approval to proceed. Completion of this project is expected by December 31, 2009.

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

The Corporation had not completed a Payment Card Industry (PCI) Data Security Standard (DSS) Self-Assessment Questionnaire (SAQ) or any other PCI DSS compliance summary plan to define its applicable vendor level and respective contractual requirements.

We found that:

- ▶ A compliance 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 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 Data Security Standard 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 interim CIO stated that the campus was aware of PCI DSS requirements but was unsure of the campus' applicable vendor level and specific requirements.

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 12**

We recommend that the Corporation and the campus:

- a. Conduct a PCI DSS assessment to determine their applicable vendor level and respective PCI requirements.
- b. Complete all PCI DSS requirements including an annual SAQ and quarterly network scans by an approved vendor, if required.

### **Campus Response**

We concur. Information technology in collaboration with the Corporation will conduct the PCI DSS Self-Assessment Questionnaire by November 30, 2009, and will work to complete all PCI DSS requirements by December 31, 2009.

## **INFORMATION SECURITY TRAINING**

Corporation, KAZU, and university advancement personnel with access to sensitive donor and financial information were not always required to complete information security awareness training.

Specifically, if personnel only had access to the donor system, they 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 training for all employees with access to critical systems or protected data.

The Corporation controller stated that information security awareness documentation was provided to employees granted PeopleSoft system access; however, this training program was not required of all employees.

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

**Recommendation 13**

We recommend that the Corporation require information security awareness training for all employees with access to critical systems or protected data.

**Campus Response**

We concur. Information technology and Corporation human resources have determined that all regular Corporation employees will be required to complete the information security awareness training provided by the chancellor's office. Corporation human resources has identified an administrator for this and enrollments will begin in July 2009.

**SYSTEM BACKUPS**

Daily, weekly, and monthly backups for Corporation systems with protected data were not encrypted when stored locally or when in transit to the off-site storage location.

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

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

The campus director of network services stated that the campus had not considered it necessary to encrypt data backups.

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

**Recommendation 14**

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

**Campus Response**

We concur. After reviewing the university's currently installed tape backup system, it was determined that encrypted backups could be performed using existing software, hardware, and tapes. Encrypted backups began on May 12, 2009. Network Services expects that all non-encrypted backups will be cycled by September 30, 2009.

**CSUMB EMPLOYEE HOUSING, INC.**

**CORPORATE GOVERNANCE**

The CSUMB Employee Housing, Inc. (CEHI) had not filed amended Articles of Incorporation with the chancellor's office in a timely manner.

We found that amendments to the Articles of Incorporation made on July 20, 2006, 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 CEHI director of operations stated that the amended Articles of Incorporations were not submitted to the chancellor's office due to oversight.

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

**Recommendation 15**

We recommend that CEHI 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 amended Articles of Incorporation were submitted to Financing and Treasury at the chancellor's office via email on December 22, 2008. This item has been added to the administrative assistant's procedure manual as a board meeting follow-up task. This recommendation was implemented in May 2009.

---

## **APPENDIX A: PERSONNEL CONTACTED**

### **Name**

### **Title**

#### **CAMPUS**

Dianne F. Harrison	President
George Ball	Property Coordinator
John Fitzgibbon	Associate Vice President of Finance
Francine Flores	Development Systems Analyst, University Advancement
Monica Galligan	Human Resources Systems Manager
Chip Lenno	Interim Chief Information Officer
Christine Limesand	Assistant Director, Grants and Contracts
Cindy Lopez	Director, Grants and Contracts
James Main	Vice President, Administration and Finance
Steven Mann	Senior Operations Analyst, Network Services
Susan McFarlane	Manager, Financial Information Systems
William Musselman	Director, Accounting
Eva Salas	Buyer
Eric Simoni	Associate Director, Information Systems
Chris Taylor	Director, Network Services
Richard Westing	Advancement Services Manager

#### **UNIVERSITY CORPORATION AT MONTEREY BAY**

Warda Alhadi	Office Manager, KAZU Radio Station (KAZU)
Sherry Baggett	Controller
Pat Clausen	Manager, Conference and Event Services
Maria Garcia	Director, Operations
Allison Griffin	Administrative and Financial Coordinator, Residential Life
Gehane Kiama	Human Resources Manager
Sharnie Mangubat	Administrative Assistant
Douglas McKnight	General Manager, KAZU
Bella Morgenstern	Accounts Payable Technician
Cordelia Ng	General Ledger Accountant
Mercedes Richter	Payroll Technician
Monica Rodriguez	Accounting Manager
Victor Salas	Accounts Payable Technician
Kevin Saunders	Executive Director
Geena Valenzuela	Human Resources Specialist
Lena Vasquez	Executive Assistant
Lorena Villalobos	Junior Accountant

#### **CSUMB EMPLOYEE HOUSING, INC.**

Maria Garcia	Director, Operations
Kevin Saunders	Managing Director

## **STATEMENT OF INTERNAL CONTROLS**

### **A. INTRODUCTION**

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

### **B. INTERNAL CONTROL DEFINITION**

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

#### **1. Internal Accounting Controls**

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

#### **2. Operational Controls**

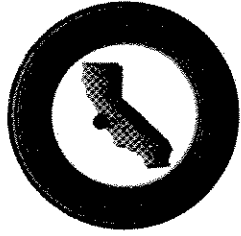
Operational controls comprise the plan of organization and all methods and procedures that are concerned mainly with operational efficiency and adherence to managerial policies and usually relate only indirectly to the financial records.

### **C. INTERNAL CONTROL OBJECTIVES**

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

**D. INTERNAL CONTROL SYSTEMS LIMITATIONS**

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



CALIFORNIA STATE UNIVERSITY  
**Monterey Bay**

OFFICE OF THE VICE PRESIDENT  
 FOR ADMINISTRATION AND FINANCE

100 CAMPUS CENTER, BUILDING 840  
 SEASIDE, CA 93955-8001  
 831-582-3398  
 FAX 831-582-3339  
 WWW.CSUMB.EDU

25 June 2009

Larry Mandel, University Auditor  
 California State University  
 Office of the University Auditor  
 401 Golden Shore, 4<sup>th</sup> Floor  
 Long Beach, CA 90802-4210

RECEIVED  
 UNIVERSITY AUDITOR

JUN 30 2009

THE CALIFORNIA STATE  
 UNIVERSITY

RE: Response to Auxiliary Organizations Audit Report  
 California State University, Monterey Bay – Report Number 08-53

In accordance with the policies and procedures for the Office of the University Auditor, enclosed please find the response to recommendations one through fifteen of audit number 08-53, Auxiliary Organizations of California State University, Monterey Bay.

Your audit has provided the campus and the auxiliary organizations with valuable management information that we will use to institute changes and improvements in our campus operations. We appreciate the effort you and your staff have made to indicate areas where our procedures or internal controls could be strengthened. The campus and the auxiliary organizations are committed to addressing and resolving the issues identified in the audit report.

Questions regarding the responses may be directed to Maria A.Y. Garcia at (831) 582-5027 or maria\_a.y.\_garcia@csumb.edu.

Sincerely,

James E. Main  
 Vice President for Administration and Finance

Enclosure

Cc (with encl.): Dianne F. Harrison, CSUMB President  
 Kevin R. Saunders, University Corporation Executive Director  
 Maria A.Y. Garcia, Director of Operations for Auxiliary Corporations  
 Sherry Baggett, University Corporation Controller  
 Chip Lenno, CSUMB Chief Information Officer  
 John Fitzgibbon, CSUMB Associate Vice President for Finance

**Audit Responses**  
**Auxiliary Organizations Report #08-53**  
**California State University, Monterey Bay**

**CAMPUS: FEES, REVENUES, AND RECEIVABLES**

The administration of Corporation matching gifts required improvement.

**Recommendation 1**

We recommend that the campus develop a matching gifts form or other method to document matching gift processing and the review of donor terms prior to the deposit of matching funds to a specifically directed recipient.

**Campus Response**

We concur. The Corporation will develop a matching gifts form or other method to document matching gift processing and the review of donor terms prior to the deposit of such gifts. This will be completed by 31 August 2009

**CAMPUS: PURCHASING AND ACCOUNTS PAYABLE**

Campus oversight of purchasing activities performed by a third-party property management firm for the Corporation student housing and CEHI employee housing was not adequate.

**Recommendation 2**

We recommend that the campus work in conjunction with the Corporation and CEHI to develop and implement procedures for oversight of purchasing activities. Such oversight should require the property management firm to submit supporting vendor invoices and Corporation and CEHI management to perform a documented review/reconciliation.

**Campus Response**

We concur. The Corporation and CEHI will work in conjunction with the campus to develop and implement procedures for oversight of purchasing activities performed by the third-party property management firms. These procedures will include a documented review/reconciliation of supporting vendor invoices provided by the third-party property management firm. The procedures will be implemented by 31 October 2009.

**CORPORATION: OPERATING AND ADMINISTRATIVE AGREEMENTS**

Certain agreements among the Corporation, the CSU Trustees, and the campus did not include appropriate indemnification clauses.

- Operating agreement did not specifically indemnify the campus
- Administrative Services agreement did not specifically indemnify the State of California and the CSU.

**Recommendation 3**

We recommend that the Corporation amend the cited agreements to include appropriate indemnification clauses and ensure that future agreements include appropriate indemnification clauses.

**Campus Response**

We concur. The cited agreements will be amended to include the appropriate indemnification clauses. This will be completed by 31 August 2009. Future agreements will include appropriate indemnification clauses.

**Audit Responses**  
**Auxiliary Organizations Report #08-53**  
**California State University, Monterey Bay**

**CORPORATION: CORPORATION GOVERNANCE**

The Corporation had not filed amended Articles of Incorporation with the chancellor's office in a timely manner.

**Recommendation 4**

We recommend that the Corporation 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 amended articles of incorporation were submitted to Financing and Treasury at the Chancellor's Office via email on 22 December 2008. This task has been added to the Administrative Assistant's procedure manual as a board meeting follow-up task. This recommendation was implemented in May 2009.

**CORPORATION: OPERATIONAL COMPLIANCE**

The Corporation did not ensure that KAZU developed policies and procedures to address the accounting and processing of cash receipts/handling and accounts receivable.

**Recommendation 5**

We recommend that the Corporation ensure that KAZU develop written policies and procedures to address the accounting and processing of cash receipts/handling and accounts receivable.

**Campus Response**

We concur. The Corporation will develop written procedures for KAZU to address the accounting and processing of cash receipts/handling and accounts receivable. The procedures will be implemented by 31 October 2009.

**CORPORATION: SEGREGATION OF DUTIES**

Duties and responsibilities over certain payroll functions were not properly segregated at the Corporation. This is a repeat finding from the prior auxiliary organizations audit.

**Recommendation 6**

We recommend that the Corporation ensure that payroll functions are properly segregated or institute mitigating procedures approved by the campus chief financial officer.

**Campus Response**

We concur. The Corporation has properly segregated payroll functions. The HR/Accounting administrative assistant receives timesheets and verifies hours. Then, the payroll technician enters hours worked as part of the payroll process. The Corporation controller or her designee verifies payroll. Human resources staff receives the checks prior to disbursement. This recommendation was implemented in May 2009.

**Audit Responses**  
**Auxiliary Organizations Report #08-53**  
**California State University, Monterey Bay**

**CORPORATION: FEES, REVENUES, AND RECEIVABLES**

Forms containing credit card information from KAZU donors were not stored in a locked cabinet with controlled access.

**Recommendation 7**

We recommend that the Corporation ensure that KAZU properly safeguards forms containing donor credit card information.

**Campus Response**

We concur. KAZU now properly safeguards forms containing donor credit card information by requiring this information to be in the possession of a KAZU employee at all times and to be locked in a cabinet in a locked office overnight. This recommendation was implemented in May 2009.

**CORPORATION: AUXILIARY PROGRAMS**

Sub-recipient monitoring was not always adequate, and formal policies and procedures for sub-recipient monitoring of contracts and grants were inadequate at the Corporation.

**Recommendation 8**

We recommend that the Corporation:

- a. Complete a proper review of the two sub-recipients that had not provided A-133 reports.
- b. Strengthen its policies and procedures to ensure the timely request, receipt, review of A-133 audit reports, and resolution of applicable findings prior to the granting of federally funded sub-awards to the sub-recipients.

**Campus Response**

We concur.

- a. The Corporation will complete a proper review of the two sub-recipients that had not provided A-133 reports. This will be completed by 30 September 2009.
- b. The Grants & Contracts office now requires the receipt and review of A-133 audit reports and resolution of applicable findings prior to the granting of federally funded sub-awards to sub-recipients. In the absence of an A-133 report, an annual financial statement will be requested. This recommendation was implemented in May 2009.

**CORPORATION: PASSWORD SECURITY**

Password security parameters were not always adequate for Corporation systems.

**Recommendation 9**

We recommend that the Corporation reassess its security requirements and set effective password security controls and account lock-out settings for its computer systems.

**Campus Response**

We concur. Whenever possible, the University will implement strong password security based on the CSU System-wide Information Security Standards. Based on these guidelines, the following controls will be implemented:

- PeopleSoft – completed verification of password history depth setting:

## Audit Responses

### Auxiliary Organizations Report #08-53

### California State University, Monterey Bay

California State University  
Monterey Bay

#### Password Controls

Enable Signon PeopleCode

**Age**

Password Never Expires

Password Expires in  Days

Warn for  Days

Do not warn of expiration

**Account Lockout**

Maximum Logon Attempts

**Miscellaneous**

Allow password to match UserID

**Minimum Length**

Minimum Password Length

**Character Requirements**

Required Number of Specials

Required Number of Digits

**Purge Inactive User Profiles**

after:  Days

**Password History**

Number of Passwords to Retain

- Active Directory – (<http://it.csumb.edu/news.php?id-5305>) Implemented 1 June 2009.
- Raiser's Edge – (<http://forums.blackbaud.com/blogs/raisersedge/archive/2009/03/30/exciting-password-changes-on-the-hosizon.aspx>) Will be completed by 31 August 2009.

#### CORPORATION: USER ACCESS REVIEWS

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

#### **Recommendation 10**

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

#### Campus Response

We concur. Information Technology in collaboration with the Corporation will review and develop guidelines for information security access, to include but not limited to, approval of data access requests and management review of user access privileges. The guidelines will be implemented by 30 November 2009

## Audit Responses

### Auxiliary Organizations Report #08-53

### California State University, Monterey Bay

#### CORPORATION: PROTECTED DATA ASSESSMENT AND SECURITY

The Corporation did not perform a periodic assessment and inventory of protected information residing on its systems, and internal resources were not adequately protected.

#### **Recommendation 11**

We recommend that the Corporation:

- a. Conduct an assessment and inventory of protected information, and ensure that a reassessment is completed, at least annually. Such an assessment would reference applications, servers/systems, databases, storage locations, protected data types, approximations for number of protected data files, existing security controls, interfaces with other systems, custodians of record, technical security offices, and individual permitted access
- b. Properly secure all systems and servers containing protected data
- c. Evaluate the feasibility of implementing a DMZ to separate and protect internal campus resources from Internet-accessible devices

#### Campus Response

We concur.

- a. Information Technology in collaboration with the Corporation will work to define, assess and secure protected data residing in auxiliary systems and university file servers. This assessment will be conducted on an annual basis. A review of the ADP payroll system will be completed by 31 August 2009 and all attempts will be made to ensure the application complies with the security policy.
- b. A review of physical and virtual security is underway by Network Services at this time. Currently all university owned systems are physically secured in an access restricted facility in building 41A. Virtual security is addressed below.
- c. At this time most campus servers are protected by software firewalls that filter sensitive TCP/UDP ports from campus and external access. The current edge dual Juniper ISG 2000 firewalls filter traffic to internal campus servers based on source, destination and TCP/UDP ports. Traffic originating from the residential network (including dormitories and the cable modem system) is physically separated from the campus using firewalls so that every transaction is filtered through the edge firewalls as well. At this time the Network Services group is developing a server security DMZ implementation plan. This plan will include separate DMZ zones for database, applications and web front-end applications. Servers will be placed in their own specific IP subnets by function and their traffic will transverse the firewall from one zone to the other. The plan is part of the ITRP2 project that will provide two Juniper ISG2000 firewalls that will be used for the DMZ zones and control internal and external user access to servers and intra-zone server communications. Network Services has completed the necessary design and implementation plans and is awaiting Chancellor's Office approval to proceed. Completion of this project is expected by 31 December 2009.

#### CORPORATION: PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

The Corporation had not completed a Payment Card Industry (PCI) Data Security Standard (DSS) Self-Assessment Questionnaire (SAQ) or any other PCI DSS compliance summary plan to define its applicable vendor level and respective contractual requirements.

#### **Recommendation 12**

We recommend that the Corporation and the campus:

- a. Conduct a PCI DSS assessment to determine their applicable vendor level and respective PCI requirements

**Audit Responses**  
**Auxiliary Organizations Report #08-53**  
**California State University, Monterey Bay**

- b. Complete all PCI DSS requirements including an annual SAQ and quarterly network scans by an approved vendor, if required

**Campus Response**

We concur. Information Technology in collaboration with the Corporation will conduct the PCI-DSS Self-Assessment Questionnaire by 30 November 2009 and will work to complete all PCI-DSS requirements by 31 December 2009.

**CORPORATION: INFORMATION SECURITY TRAINING**

Corporation, KAZU, and university advancement personnel with access to sensitive donor and financial information were not always required to complete information security awareness training.

**Recommendation 13**

We recommend that the Corporation require information security awareness training for all employees with access to critical systems or protected data.

**Campus Response**

We concur. Information Technology and Corporation Human Resources have determined that all regular Corporation employees will be required to complete the Information Security Awareness Training provided by the Chancellor's Office. Corporation Human Resources has identified an administrator for this and enrollments will begin in July 2009.

**CORPORATION: SYSTEM BACKUPS**

Daily, weekly, and monthly backups for Corporation systems with protected data were not encrypted when stored locally or when in transit to the off-site storage location.

**Recommendation 14**

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

**Campus Response**

We concur. After reviewing the University's currently installed tape backup system, it was determined that encrypted backups could be performed using existing software, hardware, and tapes. Encrypted backups began on 12 May 2009. Network Services expects that all non-encrypted backups will be cycled by 30 September 2009.

**CEHI: CORPORATION GOVERNANCE**

CEHI had not filed amended Articles of Incorporation with the chancellor's office in a timely manner.

**Recommendation 15**

We recommend that CEHI 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 amended articles of incorporation were submitted to Financing and Treasury at the Chancellor's Office via email on 22 December 2008. This item has been added to the Administrative Assistant's procedure manual as a board meeting follow-up task. This recommendation was implemented in May 2009.

THE CALIFORNIA STATE UNIVERSITY  
OFFICE OF THE CHANCELLOR



BAKERSFIELD

August 4, 2009

CHANNEL ISLANDS

CHICO

**MEMORANDUM**

DOMINGUEZ HILLS

TO: Mr. Larry Mandel  
University Auditor

EAST BAY

FROM: Charles B. Reed  
Chancellor

FRESNO

FULLERTON

SUBJECT: Draft Final Audit Report 08-53 on *Auxiliary Organizations*,  
California State University, Monterey Bay

HUMBOLDT

LONG BEACH

In response to your memorandum of August 4, 2009, I accept the response as submitted with the draft final report on *Auxiliary Organizations*, California State University, Monterey Bay.

LOS ANGELES

MARITIME ACADEMY

MONTEREY BAY

CBR/amd

NORTHRIDGE

Enclosure

POMONA

c: Dr. Dianne F. Harrison, President  
Mr. James E. Main, Vice President, Administration and Finance

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS