

FISMA

SAN JOSÉ STATE UNIVERSITY

Report Number 02-10

June 13, 2003

Members, Committee on Audit

Shailesh J. Mehta, Chair
Kyriakos Tsakopoulos, Vice Chair
William Hauck Dee Dee Myers
Erene S. Thomas Anthony M. Vitti

Staff

University Auditor: Larry Mandel
Senior Director: Janice Mirza
IS Audit Manager: Greg Dove
Senior Auditor: John Stegall

BOARD OF TRUSTEES

THE CALIFORNIA STATE UNIVERSITY

CONTENTS

INTRODUCTION

Purpose.....	1
Scope and Methodology	1
Background.....	2
Opinion	3
Executive Summary	4

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Cash Receipts.....	6
Uncleared Collections	6
Segregation of Duties	7
Revolving Fund.....	8
Payroll and Personnel.....	9
Fiscal Information Technology.....	10
CashNet System	10
Web Purchasing System.....	13
Trust Funds.....	15
Trust Fund Balances	15
Administration.....	16
Trust Expenditures	17

APPENDICES

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

ABBREVIATIONS

CSU	California State University
DRP	Disaster Recovery Plan
EO	Executive Order
FISMA	Financial Integrity and State Manager's Accountability Act
IT	Information Technology
SAM	State Administrative Manual
SJSU	San José State University
SUAM	State University Administrative Manual

INTRODUCTION

PURPOSE

The principal audit objective was to assess the adequacy of controls and systems to ensure that:

- ▶ Cash receipts are processed in accordance with laws, regulations, and management policies.
- ▶ Receivables are promptly recognized and balances are periodically evaluated.
- ▶ Purchases are made in accordance with laws, regulations, and management policies.
- ▶ Revolving fund disbursements are authorized and processed in accordance with laws, regulations, and management policies.
- ▶ Cash disbursements are properly authorized and made in accordance with established procedures, and adequate segregation of duties exists.
- ▶ Payroll/personnel criteria for hiring employees, establishing compensation rates, and authorizing disbursements are controlled, and access to personnel and payroll records and processing areas are restricted.
- ▶ Purchase and disposition of fixed assets are controlled, and assets are promptly recorded in the subsidiary records.
- ▶ Physical computer controls are in place and functioning.
- ▶ Investments are adequately controlled and securities are safeguarded.
- ▶ Trust funds are established in accordance with State University Administrative Manual (SUAM) guidelines.

SCOPE AND METHODOLOGY

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 year 2001-2002 was the primary period reviewed. In certain instances, we were concerned with representations of the most current data—in such cases, the test period was July 2002 to January 2003. Our primary focus was on internal controls. Specifically, we reviewed and tested:

- ▶ Procedures for receipting and storing cash, segregation of duties involving cash receipting, and recording of cash receipts.

INTRODUCTION

- ▶ Establishment of receivables and adequate segregation of duties regarding billing and payment of receivables.
- ▶ Approval of purchases, receiving procedures, and reconciliation of expenditures to State Controller's balances.
- ▶ Limitations on the size and types of revolving fund disbursements.
- ▶ Use of petty cash funds, periodic cash counts, and reconciliation of bank accounts.
- ▶ Authorization of personnel/payroll transactions and accumulation of leave credits in compliance with state policies.
- ▶ Posting of the property ledger, monthly reconciliation of the property to the general ledger, and physical inventories.
- ▶ Access restrictions to automated accounting systems and proper documentation of the systems.
- ▶ Procedures for initiating, evaluating, and accounting for investments.
- ▶ Establishment of trust funds, separate accounting, adequate agreements, and annual budgets.

We have not performed any auditing procedures beyond the date of our report. 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.

BACKGROUND

In 1983, the California Legislature passed the Financial Integrity and State Manager's Accountability Act of 1983 (FISMA). This act required state agencies to establish and maintain a system of internal accounting and administrative control. To ensure that the requirements are fully complied with, the head of each agency is required to prepare and submit a report on the adequacy of the system of internal accounting and administrative control following the end of each odd-numbered fiscal year. The Office of the University Auditor of the California State University (CSU) is currently responsible for conducting such audits within the CSU.

This report represents our biennial review.

OPINION

We visited the San José State University (SJSU) campus from December 9, 2002, through February 7, 2003, and made a study and evaluation of the accounting and administrative controls in effect as of February 7, 2003. Our study and evaluation were conducted in accordance with the *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.

SJSU management is responsible for establishing and maintaining adequate internal control. This responsibility, in accordance with Government Code, Sections 13402 et seq., includes documenting internal control, communicating requirements to employees, and assuring that 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 accounting and administrative controls are to provide management with reasonable, but not absolute, assurance that:

- ▶ Assets are safeguarded against loss from unauthorized use or disposition.
- ▶ Transactions are executed in accordance with management's authorization and recorded properly to permit the preparation of reliable financial statements.
- ▶ Financial operations are conducted in accordance with policies and procedures established in the State Administrative Manual, Education Code, Title 5, and Trustee policy.

Our study and evaluation revealed certain conditions, which, in our opinion, could result in errors and irregularities if not corrected. Specifically, the campus did not maintain adequate internal controls over the following areas: uncleared collections, payroll receivables, the CashNet and Web purchasing systems, and trust funds. These conditions, along with other weaknesses, are described in the executive summary and body of this report.

In our opinion, except for the effect of the weaknesses described above, the SJSU accounting and administrative controls in effect as of February 7, 2003, taken as a whole, were sufficient to meet the objectives stated above.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls change 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.

EXECUTIVE SUMMARY

The purpose of this section is to provide 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.

CASH RECEIPTS [6]

UNCLEARED COLLECTIONS [6]

Uncleared collections were not reviewed and cleared timely. Timely clearing of collection amounts reduces the risk that errors and irregularities will not be detected and the potential for improper use of these funds.

SEGREGATION OF DUTIES [7]

Collection, cash accounting, and recording duties for Spartan Daily advertising revenue were not properly segregated. Adequate segregation of duties over revenues reduces the risk of errors, irregularities, and misappropriation.

REVOLVING FUND [8]

Controls over payroll receivables did not ensure timely recovery. Prompt recovery of payroll receivables increases the likelihood of collection and improves cash flow.

PAYROLL AND PERSONNEL [9]

Campus separation procedures did not ensure documentation of the separation process and had not been finalized. Adequately controlling employee separations reduces the risk of loss and the inappropriate use of state resources.

FISCAL INFORMATION TECHNOLOGY [10]

CASHNET SYSTEM [10]

System access control and computer room physical security weaknesses were found, and an information technology (IT) disaster recovery plan (DRP) was not in place. Effective system access and computer room physical security controls reduce the risk of unauthorized access and/or accidental or malicious damage or theft to equipment and data, while a comprehensive IT DRP assures timely restoration of computer operations in the event of a disaster.

WEB PURCHASING SYSTEM [13]

Computer room physical security, user access, and backup tape storage weaknesses were found. Adequate control over computer room fire prevention/intrusion detection, user access privileges, and offsite retention of media reduces the risk of unauthorized access and/or accidental or malicious damage or theft to equipment and data.

TRUST FUNDS [15]

TRUST FUND BALANCES [15]

Forty trust accounts had negative cash balances totaling \$17,765,375 as of December 31, 2002. Adequate oversight of trust projects reduces the risk of monetary loss and positively impacts cash flow.

ADMINISTRATION [16]

Balances of student fee based trust accounts were increasing without any apparent justification. Documenting the planned use of student fee based trust funds mitigates student concerns and adverse publicity concerning the need for such fees.

TRUST EXPENDITURES [17]

Trust fund expenditures were not always properly approved. Properly approved trust expenditures reduce the risk of inappropriate expenditures and loss.

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

CASH RECEIPTS

UNCLEARED COLLECTIONS

Uncleared collections were not reviewed and cleared timely.

We noted \$15,352 in debit balances within the uncleared collections account as well as the following aged uncleared collection items:

<u>Uncleared Collections</u>	
<u>Year</u>	<u>Amount</u>
1998	\$12,316
2000	10,584
2001	7,595
2002	<u>4,558</u>
Total	<u>\$35,053</u>

State Administrative Manual (SAM) §10452 states, in part, that this account shows the amount of cash collections being checked to determine if they are to be accepted for a fund in the State Treasury or are to be refunded to payers and a representation of the types of reimbursements that must be applied at the time they are ordered into the State Treasury.

SAM §10508 states, in part, that varying circumstances determine the clearance of uncleared collections and indicates that items should be cleared at least once each quarter.

The cashiering services manager stated that letters were sent to the companies that issued the checks requesting their assistance in identifying the funds, but there have been few responses.

Untimely clearance of collection items increases the risk that errors and irregularities will not be detected and the potential for improper use of these funds.

Recommendation 1

We recommend that the campus:

- a. Research and clear the collection items cited and strengthen procedures to ensure that uncleared collections are resolved in a timely manner.
- b. Determine the cause of debit balances within the uncleared collections account and adjust them accordingly.

Campus Response

- a. We concur. Uncleared collections from multiple areas were merged to one account when PeopleSoft was implemented, making the entries difficult to identify. Last week, the balances were segregated to each respective area making it much easier to research in the future. As of June 30, 2003, fund 250002 was \$370.00 and currently has a zero balance. Effective immediately, the bursar's office will monitor this account monthly and transfer monies in a timely manner.
- b. We concur. We have identified the cause of the debit balances and adjustments are being made.

SEGREGATION OF DUTIES

Collection, cash accounting, and recording duties for Spartan Daily advertising revenue were not properly segregated.

We noted that one person performed the following duties:

- ▶ Prepared vendor billings.
- ▶ Received vendor payments.
- ▶ Forwarded collections to central cashiering for bank deposits.
- ▶ Posted vendor payments to accounting records.
- ▶ Made adjustments to vendor accounts.

SAM §8080, §8080.1, and §8080.2 state, in part, that no one person will perform more than one of the following types of duties: receiving and depositing remittances, initiating or preparing invoices, inputting receipts information, and maintaining books of original entry.

SAM §20050 states that the elements of a satisfactory system of internal accounting and administrative controls shall include a plan of organization that provides segregation of duties appropriate for proper safeguarding of state assets.

The faculty advisor responsible for management oversight of the Spartan Daily stated that it was a small operation and the cost of instituting the controls would be prohibitive.

Inadequate segregation of duties over revenues increases the risk of errors, irregularities, and misappropriation.

Recommendation 2

We recommend that the campus establish controls to ensure the appropriate segregation of duties or establish mitigating controls where incompatible duties occur.

Campus Response

We concur. We will design a system to segregate cash handling from recording and accounting duties, with sufficient oversight to compensate for any incompatible duties. This plan will be in place by September 30, 2003.

REVOLVING FUND

Controls over payroll receivables did not ensure timely recovery.

Our review of ten outstanding payroll and salary advance receivables disclosed that the campus was unable to provide documentation of collection efforts in six instances. As of December 2, 2002, we noted the following outstanding payroll receivables:

<u>Payroll Receivables</u>	
<u>Year</u>	<u>Amount</u>
1995	\$2,925
1997	107
1998	9,777
1999	5,373
2000	13,754
2001	55,731
2002	<u>98,561</u>
Total	<u>\$186,228</u>

SAM §8776.7 requires reimbursement to the state of overpayments made to employees. It further provides that any amount owed to the state by an employee is the equivalent of an overpayment and prescribes policies and procedures to be followed when collecting employee overpayments, including written notices.

State University Administrative Manual (SUAM) §3813 indicates that salary advances to employees should be collected when a corrected or delayed warrant for the pay period involved is received with the time period for recovery of salary advances not to exceed 60 days.

The payroll services manager indicated that the campus had exhausted all collection efforts for the older accounts but documentation of collection efforts was lost. She further noted that some payroll receivables involved benefit payments and the payroll staff lacked the knowledge to resolve the items.

Failure to pursue prompt recovery of payroll receivables reduces the likelihood of collection and negatively impacts cash flow.

Recommendation 3

We recommend that the campus investigate and resolve the old outstanding receivables and strengthen controls over the ongoing recovery of payroll receivables.

Campus Response

We concur. We have resolved all outstanding receivables as of May 31, 2003. Additionally, we have implemented new procedures to ensure control over the ongoing recovery of payroll receivables. The procedures were effective February 2003.

PAYROLL AND PERSONNEL

Campus separation procedures did not ensure documentation of the separation process and had not been finalized.

Our review of five employee separations, including four part-time temporary faculty and one student assistant, disclosed that clearance forms were not on file. Additionally, we noted that although guidelines for employee separations, including employee clearance procedures, had been drafted, the guidelines had not been formally approved and distributed throughout the campus.

SAM §8580.4 describes the need for adequate separation procedures, including preparation of a clearance form that includes clearance of revolving fund advances (travel and salary), return of keys, equipment, credit cards, etc.

SAM §4842.2 states, in part, the need for termination procedures that ensure that agency information assets are not accessible to former employees.

The manager of personnel services indicated that the absence of approved guidelines for employee separations and the absence of leverage, as in prior years, to hold the final paycheck had diminished the effectiveness of the department in obtaining employee separation documents.

Inadequate control over employee separations increases the risk of loss and the inappropriate use of state resources.

Recommendation 4

We recommend that the campus:

- a. Finalize and distribute the guidelines for employee separations.
- b. Establish procedures to ensure that clearance forms are prepared and retained for all separations from employment.

Campus Response

- a. We concur. On February 19, 2003, the separation guidelines were faxed to the auditor. In the first week of May 2003, the new guidelines were communicated with the campus human resources representatives for implementation within the departments. The guidelines are now posted on our human resources website.
- b. We concur. A procedure is now in place to ensure that departments assist us in the clearing of employees upon separation. The separation guidelines address specifically the preparation and retention of clearance forms.

FISCAL INFORMATION TECHNOLOGY

CASHNET SYSTEM

System access control and computer room physical security weaknesses were found, and an information technology (IT) disaster recovery plan (DRP) was not in place.

UNIX Controls and Vendor Access

Access controls to the UNIX Root account were not sufficiently restricted to prevent unauthorized access to programs and data by vendors.

SAM §4841 requires state agencies to provide for the proper use and protection of its information assets by establishing appropriate policies and procedures for preserving the integrity and security of automated files and databases.

The network analyst for systems and technology management stated that due to the limited number of information systems personnel and the need for vendors to perform contractual maintenance, total regulation of vendor activities was not possible.

Computer Physical Security

Physical security over the CashNet computer room required improvements to access, fire prevention, and intrusion detection.

We noted the following control weaknesses:

- ▶ Keys to the doors were dispersed to various departments, which may not adequately prevent unauthorized access.
- ▶ After-hour intrusion detection equipment was not installed to alert security personnel of unauthorized access.
- ▶ Fire suppression devices specific to minimizing damage to electrical equipment were not located

in close proximity to the computer room, and campus personnel had not been trained in their usage.

SAM §4842.2 requires each state agency to establish and maintain physical security measures that provide for management control of physical access to information assets. Physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility.

The network analyst for systems and technology management stated that additional equipment from other departments had recently been added to the computer room requiring additional keys to be issued; however, the security and environmental provisions in light of those changes had not been recently examined.

Disaster Recovery Planning

An IT DRP was not in place for the CashNet system.

SAM §4843.1 requires each state agency to establish and maintain both an operational recovery plan to protect its information assets in the event of a disaster or serious disruption to its operations and a plan to resume operation following a disaster affecting those applications.

Executive Order (EO) No. 696, *Implementation of The California State University Emergency Preparedness Program*, dated January 29, 1999, states, in part, that each campus president is delegated the responsibility for the implementation of an emergency management system program on campus and shall ensure that management activities including, but not limited to, maintenance and regular updating of the institutional emergency management system plan and determination, acquisition, and maintenance of facilities, equipment, and related supplies required for emergency preparedness are accomplished.

The network analyst for systems and technology management stated that the CashNet system was not supported by information systems and computing and, as such, was not included in the IT DRP.

Ineffective system access and computer room physical security controls increase the risk of unauthorized access and/or accidental or malicious damage or theft to equipment and data, while the lack of a comprehensive IT DRP may prevent the timely restoration of computer operations in the event of a disaster.

Recommendation 5

We recommend that the campus:

- a. Restrict access to the UNIX Root account and implement procedures to control vendor access when updating production copies of programs and data, where possible, or consider disconnecting the phone modem or network access and permitting such access only after formal notification by the vendor that maintenance will be performed that includes a detailed list of changes to be made.

- b. Review the need for various departments to have keys to the computer room and restrict the distribution of keys, accordingly; obtain intrusion detection devices to monitor access to the computer room during non-business hours; and install fire suppression devices specific to minimizing damage to electrical equipment.
- c. Develop an IT DRP for the CashNet system, which includes, at a minimum, contracts for hardware replacement and an alternate recovery site that reflects the status of data files at the time of restoration; and a written manual of operating and recovery procedures for business units to assist operations during an extended outage of data processing services (e.g., for the recreation of up to one week of lost data and procedures for entering data collected manually during a prolonged system outage, etc.); and determine whether weekly off-site storage of tapes is sufficient to adequately recover campus business operations. Develop an IT DRP for the CashNet system, which includes, at a minimum, contracts for hardware replacement and an alternate recovery site that reflects the status of data files at the time of restoration; and a written manual of operating and recovery procedures for business units to assist operations during an extended outage of data processing services (e.g., for the recreation of up to one week of lost data and procedures for entering data collected manually during a prolonged system outage, etc.); and determine whether weekly off-site storage of tapes is sufficient to adequately recover campus business operations.

Campus Response

- a. We concur. When assistance is needed by the bursar's office to resolve a problem, it is imperative for Informed Decisions (the cashiering system's vendor), to have this access. It is impractical to restrict the root password while the vendor is resolving system issues and problems for the bursar's office: they need to be able to provide information and resolution to the problem continuously. However, the root password will be changed after the vendor has finished solving a problem; we have implemented the changing of the root password after Informed Decisions completes work using the temporary ID assigned.
- b. We concur. Servers and other hardware are contained in separate cages within one dedicated room to assure optimum logistics and performance. Each department has possession of keys only for the access to their respective equipment. Access to the CASHNet system is accessible only by entering the bursar's office, which has a sophisticated alarm system. We will add razor barbed wire to the top of the fence to prevent intruders from climbing into the CASHNet server and the network switch areas. We will also install dedicated fire extinguishers in easily accessible locations in the proximity of the server and the network switch. These improvements are to be completed by September 30, 2003.
- c. We concur.

Coverage for CASHNet server hardware and system: We are searching for a vendor with whom to sign a system maintenance agreement to cover the replacement of hardware and to reinstall CASHNet in case of catastrophic system failure. We will have this coverage by September 30, 2003.

CASHNet System Disaster Recovery Plan: We will formally write up the Disaster Recovery Plan for CASHNet by September 30, 2003. Background: CASHNet is not considered a mission critical system, in that it feeds directly into PeopleSoft's student records, thus leaving a separate retrievable set of information that can be used for re-entering data if necessary. Also, PeopleSoft and various web tables pick up the full day's information, so the recovery issue is only with the crash day's data, and this can be re-entered manually. In addition, for many of the transactions, there is a printed paper copy (that is sent to account payable or procurement). Thus, the loss data in a crash can be retrieved/reconstructed, and the methodology for recovery will be detailed in the system disaster recovery plan.

WEB PURCHASING SYSTEM

Computer room physical security, user access, and backup tape storage weaknesses were found.

Business Systems Computer Room Physical Security

Physical security of the Web purchasing system required improvements to fire prevention and intrusion detection.

SAM §4842.2 requires each state agency to establish and maintain physical security measures that provide for management control of physical access to information assets. Physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility.

The network analyst for systems and technology management stated that the computer room has only recently been used for processing of production information and that after hour security and environmental provisions had not been recently examined.

User Access Privileges

Security administrators were not consistently notified of changes in employment status to affect changes in or removal of system access privileges.

SAM §4842.2 states that appropriate risk management procedures should be implemented to safeguard the integrity of data files, which includes effective account and password management. Effective password management is considered to include an appropriate and enforced frequency of password changes and automatic disabling of inactive accounts.

The analyst/programmer stated that campus practices did not consistently include notification to the finance division administrators.

Offsite Tape Backup

Offsite storage of backup tapes was not adequate since the backup media was stored at an employee's residence.

SAM §20050 states that there should be an established system of authorization and record-keeping procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenditures.

The network analyst for systems and technology management stated that personal retention of backup tapes was the most cost-effective solution to offsite storage.

Inadequate controls over computer room fire prevention/intrusion detection and user access privileges and personal retention of offsite media increase the risk of unauthorized access and/or accidental or malicious damage or theft to equipment and data.

Recommendation 6

We recommend that the campus:

- a. Implement additional physical controls including improved door locking devices and intrusion detection devices to monitor access to the computer room during non-business hours and install fire suppression devices specific to minimizing damage to electrical equipment.
- b. Strengthen the employee separation process to ensure that appropriate information security persons are notified of all changes in employment status that affect user access privileges.
- c. Discontinue the practice of storing backup tapes at a personal residence and establish more appropriate storage arrangements such as sending the backup tapes to the campus data center.

Campus Response

- a. We concur. (1) Door locking: when we move to Clark Hall by January 2005, we will install an OmniLock on the server room to ensure that we have good tracking of entry/exit to this room. In our current environment, this was not practical and because of the move to Clark Hall, there will be no investment in this in the current modular building. (2) Fire suppression equipment: in our current environment, an elaborate dedicated fire sprinkler system in the temporary modular building (Mod C) is not an option. When we meet with the planners for Clark Hall, we will inquire about the availability of this. In the meantime, we will install fire extinguishers in easily accessible locations in the computer rooms by September 30, 2003. (3) Intrusion detection for off hours: the rooms are key locked and only a select group of individuals have access. The front door of the modular registers all entry/exit attempts. The server consoles are locked. We purchased a UPS system to be prepared for power outages. We intend to transport this UPS system to Clark Hall.

- b. We concur. For regular employees, we have instituted a process to identify terminated employees and remove their access. This is run once a week. With respect to position changes, we will programmatically identify people whose positions have changed by querying PeopleSoft human resources data. This new procedure will be officially implemented by September 15, 2003. We have already requested that central offices, who have higher level of access than departmental end users, notify us of both terminations and position changes (in the case of termination, revocation of access will occur before the employee is terminated in PeopleSoft).
- c. We concur. We have worked out a process to regularly store tapes in the cashiering safe in the student services center (SSC). We did not want our tapes to go to the data center's offsite facility because of the time required to retrieve a tape should we need it. We rotate weekly tapes to SSC so they are still on campus when we need them.

TRUST FUNDS

TRUST FUND BALANCES

Forty trust accounts had negative cash balances totaling \$17,765,375 as of December 31, 2002.

SUAM §3710.01 states, in part, that each trust project account must maintain a positive cash balance and a positive fund balance.

SUAM §3710.04 indicates that a budget submitted by persons designated in the trust agreement as project coordinator or account administrator, reviewed by appropriate campus officials, and approved by the president or designee assists in the management of trust projects.

The senior director of accounting and administrative services stated that the reasons for negative balances in the 13 largest accounts (totaling \$17,713,583) were loan agreements with overspent trust accounts totaling \$10,571,875, anticipated reimbursements and revenues totaling \$2,313,774.99, and poor account management by repeat offenders totaling \$4,827,933. He further stated that he and his staff had held conversations with repeat offenders who overspent their accounts and had instituted budgetary controls; however, the results of these discussions had not been documented, and no written procedures were in place to deal with repeat offenders.

Inadequate control over trust projects increases the risk of monetary loss and negatively impacts cash flow.

Recommendation 7

We recommend that the campus:

- a. Establish a written plan to address the negative trust fund balances.

- b. Strengthen oversight and monitoring controls for trust funds to ensure that positive trust balances are maintained including, but not limited to, the preparation and approval of an annual budget for each major trust account.

Campus Response

We concur. The campus will create a plan to address negative trust fund cash balances. This plan will include criteria as to when an annual budget is required. Additionally, we will have the trust accountant review all trust cash balances monthly and communicate with the trust fund owner and director of accounting and financial systems as appropriate. This plan will be in place by September 30, 2003.

ADMINISTRATION

Balances of student fee based trust accounts were increasing without any apparent justification.

Our review of a random sample of seven student fee based trust accounts disclosed that the trust accounts, which had been established to provide services, materials, and programs for students, had combined balances totaling \$2,346,779 at December 31, 2002; and the balances had been increasing annually over the last two years. In addition, no written plans were in place for use of the funds (i.e., to spend down the balances). The accounts reviewed included:

<u>Fee Account Name</u>	<u>Account Balance</u>
Transit	\$685,077
Health Facility	660,827
Writing Skills Testing	495,501
Recreation	188,390
Art Pantry Operations	128,700
Residential Life Association	90,741
Chemistry Pantry	<u>97,544</u>
Total	<u>\$2,346,780</u>

SUAM §3710.04 indicates a budget submitted by persons designated in the trust agreement as project coordinator or account administrator, reviewed by appropriate campus officials, and approved by the president or designee assists in the management of trust projects.

SAM §20050 states, in part, that the elements of a satisfactory system of internal accounting and administrative controls shall include an effective system of internal review.

The accountholders for these seven trust accounts stated that they had plans for using the funds that included expansion of programs and services and maintenance reserves, but acknowledged that the plans had not been documented. The senior director of accounting and administrative services indicated that discussions were held with accountholders about the large and growing trust fund balances but stated that he had no authority to require that actions be taken to reduce the fund balances.

Failure to document the planned use of growing balances for student fee based trust funds may result in student skepticism and adverse publicity concerning the need for such fees.

Recommendation 8

We recommend that the campus require trust project administrators to submit annual budgets for trust accounts with large and growing balances, which includes a written plan to support the use of large balances.

Campus Response

We concur. As part of the plan referenced in the campus response to recommendation 7, we will include criteria to determine when a trust fund cash balance is “large and growing.” Upon this determination, the trust fund owner will be required to submit a plan to support the use of the large balance. This plan will be in place by September 30, 2003.

TRUST EXPENDITURES

Trust fund expenditures were not always properly approved.

Our review of 20 trust fund expenditures disclosed that 11 expenditures had not been approved by an individual listed on the corresponding trust agreement as a person authorized to approve disbursements from the fund.

SAM §19440.1 provides that each trust account established shall be supported by documentation of the person authorized to withdraw or expend funds and specimen signatures.

The senior director of accounting and administrative services stated that the accounting software provided for the approval of transactions at the department level not the fund level thereby granting expenditure authority to persons not identified on the trust agreement.

Failure to assure that all expenditures are properly approved increases the risk of inappropriate disbursements and loss.

Recommendation 9

We recommend that the campus strengthen control procedures to ensure that trust fund expenditures are properly approved.

Campus Response

We concur. SJSU has an in-house web-based requisitioning system. The system has built-in security to ensure that only those people with department authority can approve requisitions for that department. During the FISMA audit period, we were transitioning from a paper/signature card system to this automated process. Sometimes the authorized signatures on the trust project agreements were not in synch with the approved security form for the requisition system. During the audit, there were no findings when comparing approved requisitions to the approvals on the security forms. All 11 exceptions were against the trust project agreement. We have updated our trust project agreement form to eliminate the authorized signatures section and will rely solely on the security form as the authorized signatures. These security forms are maintained by the administrative technology office, which is responsible for all PeopleSoft and related systems security. The change to the trust project form was made in March 2003. In addition, we will add to the trust project agreement a clear reference to the approved security forms by September 30, 2003.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Robert L. Caret	President
Becky Adams	Analyst/Programmer
Edmund Almazan	Manager, Accounts Receivable
Marianne Alvarez	Captain, Support Services Command, University Police Department
Marlene Anderson	Bursar
Ruben Araiza	Property Clerk
Wilma Babayan	Accountant
Shawn Bibb	Senior Director, Accounting and Administrative Systems
Amy Chan	Accounting Technician
Sooi-Mun Chan	Business Manager, Associated Students
Jenny Chang	Accountant
Richard Costello	Assistant Athletic Director
Gerald Crawford	Network Analyst, Systems and Technology Management
Alfonso De Alba	Executive Director, Associated Students
Mike Dunefsky	Director, Administrative Technology
Jean Fong	Manager, Accounts Payable
Jackie Garcia	Manager, Payroll Services
Kathy Gay	Accounting Technician, Spartan Daily
Deana Gerhard	Collections Manager
Cecilia Hoang	Administrative Analyst, Procurement Services
Marija Jakovcevic	Operations Coordinator, Bursar's Office
Barbara Keltner	Buyer
Celeste Kitagawa	Manager, Personnel Services
Clyde Lawrence	Professor, Advertising and Spartan Daily Advisor
Rose Lee	Associate Vice President, Financial and Administrative Program Planning
Dolores Lorigo	Accounting Technician, Cashiering
Norma Lorigo	Director, Procurement Services
Robert Milnes	Director, School of Art and Design
Zeljko Pavic	Director, Writing Skills Program
Rita Peth	Purchasing Manager
Paul Siegal	Director, Accounting and Financial Systems
Pamela Stacks	Chairperson, Department of Chemistry
Trang To	Accountant
Marlene Trifilo	Cashiering Services Manager
Melanie Trifilo	Travel Coordinator
Patricia Wallraven	Accounting Technician, Spartan Daily
Patricia Young	Director, Student Health Center

STATEMENT OF INTERNAL CONTROLS

A. INTRODUCTION

Internal accounting and related operational controls established by the state of California, the CSU 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 which 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 record keeping and accounting reports from those concerned with operations or asset custody, physical controls over assets, and personnel of a quality commensurate with responsibilities.

2. Operational Controls

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

C. INTERNAL CONTROL OBJECTIVES

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

D. INTERNAL CONTROL SYSTEMS LIMITATIONS

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



San José State
UNIVERSITY

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

One Washington Square
San José, CA 95192-0006
Voice: 408-924-1500
Fax: 408-924-1515

July 23, 2003

RECEIVED
UNIVERSITY AUDITOR

AUG - 1 2003

**THE CALIFORNIA STATE
UNIVERSITY**

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

Campus Response to Audit Report Number 02-10
FISMA AUDIT
San José State University

Enclosed is San José State University's response to Audit No. 02-10.
The campus is committed to addressing the issues identified in this
audit report.

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

DON W. KASSING
Vice President for Administration and Finance

Enclosure

c: Joseph N. Crowley, Interim President
Ninh Pham-Hi, Internal Audits/Special Projects

SAN JOSÉ STATE UNIVERSITY

FISMA
AUDIT REPORT NO. 02-10

CASH RECEIPTS

UNCLEARED COLLECTIONS

Recommendation 1

We recommend that the campus:

- a. Research and clear the collection items cited and strengthen procedures to ensure that uncleared collections are resolved in a timely manner.
- b. Determine the cause of debit balances within the uncleared collections account and adjust them accordingly.

Campus Response

- a. We concur. Uncleared collections from multiple areas were merged to one account when PeopleSoft was implemented, making the entries difficult to identify. Last week the balances were segregated to each respective area making it much easier to research in the future. As of 6/30/03, fund 250002 was \$370.00 and currently has a zero balance. Effective immediately, the Bursar's Office will monitor this account monthly and transfer monies in a timely manner.
- b. We concur. We have identified the cause of the debit balances and adjustments are being made.

SEGREGATION OF DUTIES

Recommendation 2

We recommend that the campus establish controls to ensure the appropriate segregation of duties or establish mitigating controls where incompatible duties occur.

Campus Response

We concur. We will design a system to segregate cash handling from recording and accounting duties, with sufficient oversight to compensate for any incompatible duties. This plan will be in place by September 30, 2003.

REVOLVING FUND

Recommendation 3

We recommend that the campus investigate and resolve the old outstanding receivables and strengthen controls over the ongoing recovery of payroll receivables.

Campus Response

We concur. We have resolved all outstanding receivables as of May 31, 2003. Additionally, we have implemented new procedures to ensure control over the ongoing recovery of payroll receivable. The procedures were effective February 2003.

PAYROLL AND PERSONNEL

Recommendation 4

We recommend that the campus:

- a. Finalize and distribute the guidelines for employee separations.
- b. Establish procedures to ensure that clearance forms are prepared and retained for all separations from employment.

Campus Response

- a. We concur. On 2-19-03 the Separation Guidelines were faxed to the auditor (John Stegall). The first week of May 2003 the new guidelines were communicated with the campus HR Representatives for implementation within the departments. The guidelines are now posted on our HR website.
- b. We concur. A procedure is now in place to ensure that departments assist us in the clearing of employees upon separation. The Separation Guidelines addresses specifically the preparation and retention of clearance forms.

FISCAL INFORMATION TECHNOLOGY

CASHNET SYSTEM

Recommendation 5

We recommend that the campus:

- a. Restrict access to the UNIX Root account and implement procedures to control vendor access when updating production copies of programs and data, where possible, or consider disconnecting the phone modem or network access and permitting such access only after formal notification by the vendor that maintenance will be performed that includes a detailed list of changes to be made.
- b. Review the need for various departments to have keys to the computer room and restrict the distribution of keys, accordingly; obtain intrusion detection devices to monitor access to the computer room during non-business hours; and install fire suppression devices specific to minimizing damage to electrical equipment.
- c. Develop an IT DRP for the CashNet system, which includes, at a minimum, contracts for hardware replacement and an alternate recovery site that reflects the status of data files at the time of restoration; and a written manual of operating and recovery procedures for business units to assist operations during an extended outage of data processing services (e.g., for the recreation of up to one week of lost data and procedures for entering data collected manually during a prolonged system outage, etc.); and determine whether weekly off-site storage of tapes is sufficient to adequately recover campus business operations.

Campus Response

- a. We concur. When assistance is needed by the Bursar's Office to resolve a problem it is imperative for Informed Decisions (the cashiering system's vendor), to have this access. It is impractical to restrict the root password while the vendor is resolving system issues and problems for the Bursar's Office: they need to be able to provide information and resolution to the problem continuously. However, root password will be changed after the vendor has finished solving a problem; we have implemented the changing of the root password after Informed Decisions completes work using the temporary ID assigned.

- b. We concur. Servers and other hardware are contained in separate cages within one dedicated room to assure optimum logistics and performance. Each department has possession of keys only for the access to their respective equipment. Access to the CASHNet system is accessible only by entering the Bursar's Office, which has a sophisticated alarm system. We will add razor barbed wire to the top of the fence to prevent intruders from climbing into the CASHNet Server and the Network Switch areas. We will also install dedicated fire extinguishers in easily accessible locations in the proximity of the server and the network switch. These improvements are to be completed by 9/30/03.
- c. We concur.
Coverage for CASHNet server hardware and system: We are searching for a vendor with whom to sign a System Maintenance Agreement to cover the replacement of hardware and to reinstall CASHNet in case of catastrophic system failure. We will have this coverage by 9/30/03.
CASHNet System Disaster Recovery Plan: We will formally write up the Disaster Recovery Plan for CASHNet by 9/30/03. Background: CASHNet is not considered a mission critical system, in that it feeds directly into PeopleSoft's student records, thus leaving a separate retrievable set of information that can be used for re-entering data if necessary. Also, PeopleSoft and various web tables pick up the full day's information, so the recovery issue is only with the crash day's data, and this can be re-entered manually. In addition, for many of the transactions, there is a printed paper copy (that is sent to Account Payable or Procurement). Thus, the loss data in a crash can be retrieved/reconstructed, and the methodology for recovery will be detailed in the System Disaster Recovery Plan.

WEB PURCHASING SYSTEM

Recommendation 6

We recommend that the campus:

- Implement additional physical controls including improved door locking devices and intrusion detection devices to monitor access to the computer room during non-business hours and install fire suppression devices specific to minimizing damage to electrical equipment.
- Strengthen the employee separation process to ensure that appropriate information security persons are notified of all changes in employment status that affect user access privileges.
- Discontinue the practice of storing backup tapes at a personal residence and establish more appropriate storage arrangements such as sending the backup tapes to the campus data center.

Campus Response

- We concur. (1) Door locking: when we move to Clark Hall by Jan 2005, we will install an OmniLock on the server room to ensure that we have good tracking of entry/exit to this room. In our current environment this was not practical, and because of the move to Clark Hall, there will be no investment in this in the current modular building. (2) Fire suppression equipment: in our current environment, an elaborate dedicated fire sprinkler system in the temporary modular building (Mod C) is not an option. When we meet with the planners for Clark Hall we will inquire about the availability of this. In the meantime, we will install fire extinguishers in easily accessible locations in the computer rooms by 9/30/03 (3) Intrusion detection for off hours: the rooms are key locked and only a select group of individuals have access. The front door of the modular registers all entry/exit attempts. The server consoles are locked. We purchased a UPS system to be prepared for power outages. We intend to transport this UPS system to Clark Hall.

- b. We concur. For regular employees we have instituted a process to identify terminated employees and remove their access. This is run once a week. With respect to position changes, we will programmatically identify people whose positions have changed by querying PeopleSoft HR data. This new procedure will be officially implemented by 9/15/03. We have already requested that central offices, who have higher level of access than departmental end users, to notify us of both terminations and position changes (in the case of termination, revocation of access will occur before the employee is terminated in PeopleSoft).
- c. We concur. We have worked out a process to regularly store tapes in the Cashiering safe in the Student Services Center (SSC). We did not want our tapes to go to the data center's offsite facility because of the time required to retrieve a tape should we need it. We rotate weekly tapes to SSC so they are still on campus when we need them.

TRUST FUNDS

TRUST FUND BALANCES

Recommendation 7

We recommend that the campus:

- a. Establish a written plan to address the negative trust fund balances.
- b. Strengthen oversight and monitoring controls for trust funds to ensure that positive trust balances are maintained including, but not limited to, the preparation and approval of an annual budget for each major trust account.

Campus Response

We concur. The campus will create a plan to address negative trust fund cash balances. This plan will include criteria as to when an annual budget is required. Additionally, we will have the Trust Accountant review all trust cash balances monthly and communicate with the trust fund owner and Director of Accounting and Financial Systems as appropriate. This plan will be in place by September 30, 2003.

ADMINISTRATION

Recommendation 8

We recommend that the campus require trust project administrators to submit annual budgets for trust accounts with large and growing balances, which includes a written plan to support the use of large balances.

Campus Response

We concur. As part of the plan referenced in the Campus Response to Recommendation 7, we will include criteria to determine when a trust fund cash balance is "large and growing". Upon this determination the trust fund owner will be required to submit a plan to support the use of the large balance. This plan will be in place by September 30, 2003.

TRUST EXPENDITURES

Recommendation 9

We recommend that the campus strengthen control procedures to ensure that trust fund expenditures are properly approved.

Campus Response

We concur. SJSU has an in-house web-based requisitioning system. The system has built in security to ensure that only those people with department authority can approve requisitions for that department. During the FISMA audit period we were transitioning from a paper/signature card system to this automated process. Sometimes the authorized signatures on the Trust Project Agreements were not in synch with the approved security form for the requisition system. During the audit there were no findings when comparing approved requisitions to the approvals on the security forms. All 11 exceptions were against the Trust Project Agreement. We have updated our Trust Project Agreement form to eliminate the Authorized Signatures section and will rely solely on the Security form as the authorized signatures. These security forms are maintained by the Administrative Technology office, which is responsible for all PeopleSoft and related systems security. The change to the Trust Project form was made in March 2003. In addition, we will add to the Trust Project Agreement a clear reference to the Approved Security Forms by September 30, 2003.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

August 6, 2003

CHANNEL ISLANDS

CHICO

MEMORANDUM

DOMINGUEZ HILLS

FRESNO

TO: Mr. Larry Mandel
University Auditor

FULLERTON

HAYWARD

FROM: Charles B. Reed
Chancellor

HUMBOLDT

LONG BEACH

SUBJECT: Draft Final Report Number 02-10 on *FISMA*,
San José State University

LOS ANGELES

MARITIME ACADEMY

In response to your memorandum of August 6, 2003, I accept the response as submitted with the draft final report on *FISMA*, San José State University.

MONTEREY BAY

NORTHRIDGE

CBR/ac

POMONA

Enclosure

SACRAMENTO

SAN BERNARDINO

cc: Dr. Joseph N. Crowley, Interim President
Mr. Don W. Kassing, Vice President for Administration and Finance

SAN DIEGO

SAN FRANCISCO

SAN JOSE

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS