

FISMA

**CALIFORNIA POLYTECHNIC STATE UNIVERSITY,
SAN LUIS OBISPO**

**Report Number 02-04
September 13, 2002**

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
Internal Auditor: Michael Perry

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.....	7
Purchasing.....	8
Revolving Fund.....	9
Payroll/Personnel	10
Fixed Assets.....	11
Physical Inventory	11
Property Records	12
Fiscal Information Technology.....	12
Disaster Recovery Plan.....	12
Program Change Control.....	16
Mainframe Security	17
PeopleSoft Security	18
User Account Removal.....	19
Vendor Access to CashNet.....	20
Reconciliations.....	21

APPENDICES

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

ABBREVIATIONS

AFD	Administration and Finance Division
Cal Poly	California Polytechnic State University
CMS	Common Management System
COBIT	Control Objectives for Information Technology
CSU	California State University
CSU Hayward	California State University, Hayward
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards
FISMA	Financial Integrity and State Manager's Accountability Act
IT	Information Technology
NIST	National Institute of Standards and Technology
SAM	State 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 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 2000-2001 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 2001 to January 2002. 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.
- ▶ 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 California Polytechnic State University (Cal Poly), San Luis Obispo campus from February 19, 2002, through April 12, 2002, and made a study and evaluation of the accounting and administrative control in effect as of April 12, 2002. 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.

Cal Poly San Luis Obispo's 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 control 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: revolving fund, payroll and personnel, and information technology. 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, Cal Poly San Luis Obispo's accounting and administrative control in effect as of April 12, 2002, 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 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 [7]

Cash controls were in need of improvement at the university police department. Adequate control over cash receipts reduces the risk of errors, irregularities, and misappropriation.

PURCHASING [8]

Procurement card transactions did not always include adequate supporting documentation. Valid detailed invoices and receipts to support procurement card transactions reduce the risk of improper or duplicate payments.

REVOLVING FUND [9]

Independent cash counts of petty cash and change funds did not always occur with the required frequency, and a change fund had been established without proper approval. The finding concerning cash counts is a repeat from the prior Financial Integrity and State Manager's Accountability Act (FISMA) audit. Cash counts conducted at prescribed frequencies and properly approved change funds reduce the risk of the loss of funds and comply with state policy.

PAYROLL/PERSONNEL [10]

Documentation of the employee separation process was not always complete. Adequate control over employee separation procedures reduces the risk of loss of state funds and the inappropriate use of state resources.

FIXED ASSETS [11]

PHYSICAL INVENTORY [11]

Physical inventories had not been completed within the prescribed frequency for two campus departments. Timely physical inventories reduce campus exposure to loss/misuse of fixed assets.

PROPERTY RECORDS [12]

Property purchases were not always communicated to university property services. Adequate control over the tagging and capitalization of property reduces the risk of misstating inventory and accounting records and of undetected loss or theft.

FISCAL INFORMATION TECHNOLOGY [12]

DISASTER RECOVERY PLAN [12]

The information technology (IT) disaster recovery plan (DRP) did not contain sufficient information to ensure that data processing services could be recovered in a timely manner. With a detailed IT DRP, corresponding business continuation procedures, and frequent off-site backup tape storage, the campus may be better able to restore computer operations and critical information within a reasonable time frame thereby reducing the impact of a disaster on normal business operations.

PROGRAM CHANGE CONTROL [14]

Existing practices did not prevent all persons with student administration programming responsibilities from making unauthorized changes to production programs and data. Internal controls are enhanced when programmers do not have the capability to make changes directly to production copies of programs and data along with authorized changes by management.

MAINFRAME SECURITY [17]

Some mainframe security (RACF) parameters were not set to provide effective protection, and many sensitive libraries were not sufficiently protected. Security parameters set to provide effective protection of programs and data files reduce the risk of unlimited access to system resources obtained through inappropriate access to sensitive libraries.

PEOPLESOFT SECURITY [18]

The security product, PentaSafe, had not been implemented to enhance password controls over the PeopleSoft application. Adequate configurations of system security software reduce the risk that unauthorized users will gain access to campus systems and confidential data.

USER ACCOUNT REMOVAL [19]

Security administration over the student administration system did not provide for deletion of revoked mainframe IDs. Deleting revoked accounts from the system prevents personnel from inappropriate access if a revoked ID is reissued to another person.

VENDOR ACCESS TO CASHNET [20]

The software vendor for the CashNet system had unlimited access to all programs and data including credit card information. Restricting vendor access to the CashNet system provides assurance to management that all changes to the software are authorized and that internal controls are not compromised.

RECONCILIATIONS [21]

INTRODUCTION

A revolving fund reconciliation had not been performed since the campus conversion to PeopleSoft in July 2001. In addition, certain application fees, fixed assets, uncleared collections, investments and bank reconciliations did not show the name of the preparer and reviewer and/or the date they were prepared and reviewed. Completing reconciliations in a timely and complete manner improves accountability and the campus' ability to detect errors and irregularities.

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

CASH RECEIPTS

Cash controls were in need of improvement at the university police department.

We found that:

- ▶ Cash receipts were transferred from the university police reception area, dispatch safe, and information booth to the cashier's office without the use of transfer receipts.
- ▶ A written record of individuals with access to the safe and the date of the last combination change was not kept for the information booth where public parking permits are sold. This is a repeat finding from the prior Financial Integrity and State Manager's Accountability Act (FISMA) audit.
- ▶ Checks received in the university police reception area were not always restrictively endorsed by the end of the day.

State Administrative Manual (SAM) §8021 requires transfer receipts to localize accountability for cash or negotiable instruments to a specific employee from the time of its receipt to its deposit.

SAM §8024 requires changing safe combinations when employees leave a department and maintaining a record listing the date the combination was last changed and the names of individuals knowing the present combination.

SAM §8023 and §8034.1 require that checks and negotiable instruments be restrictively endorsed for deposit as soon as possible after receipt, but no later than the end of the working day.

The director of fiscal services stated that she was unaware that campus procedures did not adequately satisfy the requirements for transfer receipts. She further stated that because the information booth is staffed mainly with student assistants, the risk of not changing the safe combination and maintaining related records as outlined in the SAM is outweighed by the associated costs. Additionally, she noted that the information booth is secured by a locked door and alarm system. The university police business services coordinator indicated that staff have a restrictive endorsement stamp and are aware of the endorsement requirement, but established procedures were not followed.

Inadequate control over cash receipts increases the risk of errors, irregularities, and misappropriation.

Recommendation 1

We recommend that the campus:

- a. Establish procedures to utilize transfer receipts when transferring funds from university police to the cashier's office.
- b. Maintain a record of individuals who have access to the information booth safe and the date the combination was last changed.
- c. Strengthen procedures to ensure that all checks received in the university police reception area are endorsed by the end of the day.

Campus Response

- a. We concur. The University has instituted procedures for utilization of transfer receipts when transferring funds from university police to the university cashier's office.
- b. We concur. A record of individuals who have access to the information booth safe is being maintained and stored with the university cashier's office.
- c. We concur. The university police has strengthened procedures to ensure that checks are restrictively endorsed on a daily basis. Previous noncompliance in this area was found to be on an isolated basis and additional enforcement of the existing procedures should ensure compliance.

Anticipated Completion Date: Complete.

PURCHASING

Procurement card transactions did not always include adequate supporting documentation.

Our review of six procurement card statements from February 2002 disclosed that two statements did not include itemized receipts for some transactions, and three statements used on-line confirmations or e-mails as invoices or receipts.

The California Polytechnic State University (Cal Poly), San Luis Obispo *Procurement Card Handbook* requires that an itemized receipt or invoice be obtained from vendors, attached to the monthly procurement card purchase report, and forwarded to the approving official each month. Further, an itemized receipt is required whether the purchasing transaction is made by telephone, in person, or via the Internet.

The director of contracts and procurement services indicated that the missing detailed receipts were inadvertently not provided, and he located them in the cardholders' files. He further stated that on-line confirmations are likely to be the only available documentation for some purchases.

The lack of valid detailed invoices or receipts to support procurement card transactions increases the risk of improper payments.

Recommendation 2

We recommend that the campus strengthen controls to ensure that original receipts or invoices are included in support of all procurement card purchases.

Campus Response

We concur. Emphasis will be placed on monthly submission requirements during training of cardholders. Additionally, the approving officials are being reminded that itemized invoices are required with each submission.

Anticipated Completion Date: Complete.

REVOLVING FUND

Independent cash counts of petty cash and change funds did not always occur with the required frequency, and a change fund had been established without proper approval. The finding concerning cash counts is a repeat from the prior Financial Integrity and State Manager's Accountability Act (FISMA) audit.

We reviewed independent cash counts over the past two years and found that required counts were missed at the athletic ticket office (six times); facilities services (twice); parking services (twice); university police (once); and student services (once).

In addition, we found that a change fund had been established for event parking in the university police department in the amount of \$600 without proper approval.

SAM §8111.2 states, in part, that an employee other than the custodian of the change or petty cash fund will count it in accordance with the following schedule and report the count to the accounting officer.

<u>Size of Fund</u>	<u>Frequency of Count</u>
\$200.00 or less	Annually
\$200.01 to \$500.00	Quarterly
\$500.01 to \$2,500.00	Monthly
Over \$2,500.00	At least monthly

SAM §8111.1 states that each change fund in excess of \$500 will be established only after approval of the Fiscal Systems and Consulting Unit, Department of Finance.

The director of fiscal services stated that the campus has to assess the costs and benefits of performing fund audits, including the size of the funds being audited. She further stated that there has been significant improvement in the campus performance of change fund audits. Additionally, she indicated that the event parking change fund is considered to be three separate \$200 change funds, which would not require Department of Finance approval.

Not conducting independent cash counts at prescribed frequencies and not obtaining required fund approvals increase the risk of the loss of funds and noncompliance with state policy.

Recommendation 3

We recommend that the campus strengthen procedures to count petty cash and change funds in accordance with the prescribed schedule and obtain Department of Finance approval for the event parking fund.

Campus Response

We concur. The university has strengthened procedures to ensure that petty cash and change fund counts are performed in a timely manner in compliance with SAM provisions. University cashiering personnel are performing the counts themselves to ensure the timely occurrence of counts in several of the areas. The three event parking change funds are now being maintained as completely separate change funds of \$200 each and are being counted and handled as such.

Anticipated Completion Date: Complete.

PAYROLL/PERSONNEL

Documentation of the employee separation process was not always complete.

Our review of six employee separations disclosed that a separation form was not obtained from one employee, and two employee separation forms were not fully completed. Additionally, the current employee separation form did not include an item to assure settlement of salary advances as part of the separation process.

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

The assistant director of payroll services and the interim director of human resources stated that the campus needs to assign responsibility for monitoring completion of the separation process to a single office or individual.

Inadequate control over employee separation procedures increases the risk of loss of state funds and the inappropriate use of state resources.

Recommendation 4

We recommend that the campus strengthen separation procedures to ensure that separation forms are completed for all separated employees and revise the employee separation form to assure the settlement of any salary advances.

Campus Response

We concur. The university has instituted procedures to include review and settlement of salary advances as part of the separation form and procedures. Responsibility for monitoring completion of employee separation procedures has been assigned to that office responsible for completion of other steps in the separation process for certain groups of employees.

Anticipated Completion Date: Complete.

FIXED ASSETS

PHYSICAL INVENTORY

Physical inventories had not been completed within the prescribed frequency for two campus departments.

We found that the most recent physical inventories for the computer center and facilities services were completed on November 4, 1998, and July 23, 1998, respectively, which exceeds the prescribed three-year frequency.

SAM §8652 requires departments to physically count all property at least once every three years.

The assistant director of financial reports stated that a catastrophic illness and subsequent work disability of a key staff member prevented timely completion of the computer center and facilities services property inventories. He further stated that the computer center inventory was 95 percent complete at the conclusion of audit fieldwork.

Untimely physical inventories increase campus exposure to loss/misuse of fixed assets.

Recommendation 5

We recommend that the campus complete the physical inventories of the computer center and facilities services and report the results to management.

Campus Response

We concur. The facility services inventory has been completed and the computer center inventory has been divided up into smaller, more manageable units to allow for completion of the inventories within the required time frames.

Anticipated Completion Date: December 31, 2002.

PROPERTY RECORDS

Property purchases were not always communicated to university property services.

Our review of 20 property purchases disclosed that three property acquisitions had not been added to campus property records. In addition, we found that university property services was not receiving regular notification of campus purchases requiring entry into the campus inventory system.

SAM §8650 and §8651 require that state property be recorded and tagged after acquisition.

The assistant director of financial reports stated that the items identified should have been tagged and included in campus inventory records. He further stated that the conversion to PeopleSoft and some unexpected post-conversion development efforts delayed the availability of purchasing reports used for property recording and tagging.

Inadequate control over the tagging and capitalization of property increases the risk of misstated inventory and accounting records and of undetected loss or theft.

During the course of our review, the campus completed development and implementation of an on-line property purchasing report permitting university property services to identify all property received by the campus.

FISCAL INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

The information technology (IT) disaster recovery plan (DRP) did not contain sufficient information to ensure that data processing services could be recovered in a timely manner.

The existing written data processing DRP did not address all of the required areas. For example, arrangements for an alternate facility had not been complete; the plan had not been effectively tested; and end-user recovery procedures had not been developed.

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.

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 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 director of communications and computing services stated that plans were in place to acquire the necessary hardware. She further indicated that data recovery procedures were documented for operating systems, but comprehensive, detailed recovery policies and procedures had not been completed for other systems.

Without a detailed IT DRP, corresponding business continuation procedures, and frequent off-site storage of backup tapes, the campus may not be able to restore computer operations within a reasonable time frame, which could severely impact the ability of the campus to conduct normal business operations.

Recommendation 6

We recommend that the campus:

- a. Enhance the IT DRP by adding detailed procedures for all sections outlined in SAM, develop campus business continuity plans to sustain operations during an extended outage of data processing services, and add an assumptions list that should be shared with the business users to enhance their understanding of what services will and will not be restored as part of the IT recovery plan. The assumptions list should also reflect the status of data files at the time of restoration.
- b. Conduct a business impact assessment to determine the maximum length of time that the departments could operate without data processing services, and identify the equipment and information that would be needed to sustain operations during an outage of data processing services.

- c. Develop written manual operating and recovery procedures for business units to assist operations during an extended outage of data processing services, such as manual recovery of up to one week of lost data, and procedures for entering data collected manually during a prolonged system outage.

Campus Response

- a. & b. SAM §4843 recommends the following elements in the operational recovery planning process. Responses to these elements are noted in italics.

The operational recovery planning process provides necessary preparation to design and document a sufficient set of procedures to assure continued agency operations in the event of a disaster or any other event resulting in unplanned discontinuation of IT systems operations. Each agency's process should include the following elements and culminate with the documentation of results in the form of an Operational Recovery Plan:

1. Establishment of an Operational Recovery Planning Team which will be responsible for the detailed technical analysis and planning functions that are fundamental to an operational plan.

Included in Disaster Recovery Plan—Section 4D, Recovery Team Concept provided on September 17, 2002.

2. Development of an understanding of the agency's mission, including the organizational, managerial, and technical environments within which an effective Operational Recovery Plan must work.

Included in Disaster Recovery Plan—Section 4A, Introduction provided on September 17, 2002.

3. Re-assessment of the agency's identification of the most probable types of disaster occurrences and the cost effective protective measures to be implemented, that were identified as a result of the risk management process. See SAM §4842 through 4842.21 for risk management policies.

Included in Disaster Recovery Plan—Section 4A, Introduction; 4C, Risk Assessment Summary provided on September 17, 2002.

4. Assessment of the resource requirements (equipment, communications, data, software, personnel and time) required for the agency's critical applications identified through the risk management process.

Included in Disaster Recovery Plan—Section 4E, Business Impact Analysis, and 4F, Risk Assessment provided on September 17, 2002.

5. Identification and evaluation of alternative recovery strategies.

A proposal to Cal Poly management staff in fall 2001 recommended having on-site trailers as an alternate site. Recommendation approved. Sites identified. In process of determining costs for umbilical power and network connectivity and selecting trailer provider.

Anticipated Completion Date: June 30, 2003.

6. Preparation of a cost benefit analysis for each alternative.

A proposal to Cal Poly management staff in fall 2001 recommended having on-site trailers as an alternate site. Recommendation approved. Sites identified. In process of determining costs for umbilical power and network connectivity and selecting trailer provider.

Anticipated Completion Date: June 30, 2003.

7. Selection of the alternative that best responds to the agency's requirements for disaster recovery.

A proposal to Cal Poly management staff in fall 2001 recommended having on-site trailers as an alternate site. Recommendation approved. Sites identified. In process of determining costs for umbilical power and network connectivity and selecting trailer provider.

Anticipated Completion Date: June 30, 2003.

8. Determination of specific recovery procedures and the time frame for their execution.

Included in Disaster Recovery Plan—Section 4E, Business Impact Analysis, and 4F, Risk Assessment provided on September 17, 2002.

A proposal to Cal Poly management staff in fall 2001 recommended having on-site trailers as an alternate site. Recommendation approved. Sites identified. In process of determining costs for umbilical power and network connectivity and selecting trailer provider.

Anticipated Completion Date: June 30, 2003.

9. Identification of individuals or teams within the agency that will be responsible for managing and implementing specific recovery procedures.

Included in Disaster Recovery Plan—Section 4D, Recovery Team Concept provided on September 17, 2002.

10. Documentation of the results of the planning process in the form of an Operational Recovery Plan, as specified in SAM §4843.1 and §4845.

Provided to auditors on September 17, 2002.

- c. We concur. There is a need for written procedures to assist operations during an extended outage of data processing services. Given that our data processing center backs up our data on a daily basis and creates an offsite copy, the most likely scenarios are the loss of a day's worth of activity or an extended outage of the center.

Anticipated Completion Date: March 31, 2003.

PROGRAM CHANGE CONTROL

Existing practices did not prevent all persons with student administration programming responsibilities from making unauthorized changes to production programs and data.

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 director of application and information management stated that formal, written procedures are being developed, which will include automatic audit logging of all changes made.

Since programmers have the capability to make changes directly to production copies of student administration programs and data, management cannot be assured that all changes made are authorized and, consequently, that internal controls are not compromised.

Recommendation 7

We recommend that the campus restrict all programmers from update access to production copies of programs and data or establish a detective control to identify programs that have been changed and require management to review such changes on a regular basis, as well as require specific written authorization from management for data access.

Campus Response

The information technology services department currently operates without a formal librarian role and/or librarian software application which would be needed to fully implement and meet the requirements of this recommendation. We will pursue the following:

1. Implement an automated logging process to identify programmers who compiled jobs within the production environment.
2. Review the logs on a regular basis to identify inappropriate activity.
3. Publish the current procedures for providing data access.

Anticipated Completion Date: December 31, 2002.

MAINFRAME SECURITY

Some mainframe security (RACF) parameters were not set to provide effective protection, and many sensitive libraries were not sufficiently protected.

Specifically, we noted:

- ▶ Tape DSN, which enables protection of data sets stored on tape, was not in effect.
- ▶ RACF special privileges had been granted to individuals that did not need such access to perform their job responsibilities, and some accounts in revoked status had not been deleted.
- ▶ The default password for the RVAR command had not been changed.
- ▶ Systemwide read access was provided to libraries whose names begin with high level "SYS1," which could reveal sensitive information about the system.

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 coordinator of information technology services stated that the procedures for maintaining parameter settings had been in place for several years and had not been recently examined.

Since security parameters were not set to provide effective protection, programs or data files could be created that would not be protected by RACF, information stored on magnetic tape would not be protected, and unlimited access to system resources could be obtained through inappropriate access to sensitive libraries.

Recommendation 8

We recommend that the campus:

- a. Change the aforementioned RACF settings regarding tape data set protection and the RVAR command to provide stronger security.
- b. Review the use of special privileges and ensure that they are assigned to only those individuals that require such access to perform their normal job duties.
- c. Change the universal access code setting to NONE for sensitive SYS1 libraries in order to reduce the risk of unauthorized modification or disclosure.

Campus Response

Tape DSN—Cal Poly will consult with California State University, Hayward (CSU Hayward) since this is a global RACF change that affects both campuses.

RACF SPECIAL—A review of accounts with RACF SPECIAL was conducted with these findings:

- Cal Poly and CSU Hayward share the same mainframe environment, and each campus manages security for their own resources, requiring RACF administrators at each campus with “department” SPECIAL.
- Staff members at the Cal Poly help desk have limited RACF capabilities allowing them to change Cal Poly user passwords.

Default RVAR Y password—The IBM default RVAR Y password has been changed as recommended.

One account with SPECIAL that is revoked but not deleted is IBMUSER. That account must remain on the system to support IBM upgrades. Two other accounts were requested by the auditors during the last FISMA audit and have been deleted.

Anticipated Completion Date:

Tape DSN security in WARN mode – December 1, 2002.

Tape DSN security in FAIL mode – January 1, 2003.

PEOPLESOFT SECURITY

The security product, PentaSafe, had not been implemented to enhance password controls over the PeopleSoft application.

The PeopleSoft application system did not provide robust security over password syntax and revocation. Effective practices for password management require a minimum number of password characters, enforce alphanumeric passwords, and enforce revocation of user IDs after a predetermined number of failed password attempts.

SAM §4842 states that appropriate risk management procedures should be implemented to safeguard the integrity of data files, which includes effective password management. Effective password management is considered to include an appropriate minimum password length and an appropriate and enforced frequency of password changes. See Department of Defense Password Management Guideline (a.k.a. Greenbook), the Control Objectives for Information Technology (COBIT) and Federal Information Processing Standards Publication 112 (FIPS112 and 190), and Section 3.11.3 of the Generally Accepted Principles and Practices for Securing Information Technology Systems SP 800-14 by the National Institute of Standards and Technology (NIST).

The director of administration and finance division (AFD) technology services stated that the PeopleSoft system had recently been placed into production and that the security software product was not yet available at the time of implementation.

Inadequate configurations of system security software could allow unauthorized users to gain access to campus systems and confidential data.

Recommendation 9

We recommend that the campus address the deficiencies in PeopleSoft password security either by implementing the PentaSafe software or through enhancing security through other means.

Campus Response

Cal Poly expects to implement PeopleSoft Release 8.0 for Human Resources by July 1, 2003. PeopleSoft 8.X implementation for Financials is planned for February 2004. Enhanced security for Financials 7.5 is currently under review by Common Management System (CMS) central staff, and we will implement their suggestions after they are published. Anticipated completion date: August 2003 (after completion of year-end close and contingent on development by CMS central staff).

USER ACCOUNT REMOVAL

Security administration over the student administration system did not provide for deletion of revoked mainframe IDs.

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

The director of application and information management stated that the campus had recently changed the way that users access the system eliminating the need for mainframe CICS IDs, but that the old IDs had not been removed from the system.

Leaving revoked accounts on the system represents a custodial activity, which could inadvertently lead to personnel being granted inappropriate access if a revoked ID is reissued to another person.

Recommendation 10

We recommend that the campus ensure that the process for assigning and removing IDs is consistent across all computing platforms and application systems.

Campus Response

We concur. In order to ensure that the process for assigning and removing ITS is consistent across all computing platforms and application systems, ITS is in the process of building a middleware infrastructure that will support central authentication services. This is in coordination with the statewide Middleware Initiative for the CSU.

One of the first phases of this project is to create an identity reconciliation system capable of storing necessary attributes. Once completed, ITS will encourage application administrators to utilize central authentication services against the enterprise directory.

While this will allow the pursuance of central authentication, moving the campus applications into this infrastructure will be an ongoing process.

Anticipated Completion Date: December 31, 2002.

VENDOR ACCESS TO CASHNET

The software vendor for the CashNet system had unlimited access to all programs and data including credit card information.

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 manager of AFD network and technology services stated that given the limited number of IT personnel, the system had been in place for some time and had not been recently examined.

Because vendors have the capability to make changes directly to production copies of programs and data, management cannot be assured that all changes made are authorized and, consequently, that internal controls are not compromised. In addition, the campus does not have any authority over the hiring practices of the vendor organizations to which they are granting the unlimited access rights.

Recommendation 11

We recommend that the campus:

- a. Restrict vendors from directly 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. Develop a method to prohibit access to credit card information by vendor personnel.

Campus Response

We concur.

Vendor access will be controlled via AIX account management. A procedure is being developed to enable and disable the support account. Vendor access to the system will be by request only. Access will be disabled by Cal Poly personnel after a support event.

Anticipated Completion Date: December 31, 2002.

Effective with release 5.38 of the CashNet software, the credit card information will be encrypted. Cal Poly plans to implement this release in December of 2002.

Anticipated Completion Date: December 31, 2002.

RECONCILIATIONS

A revolving fund reconciliation had not been performed since the campus conversion to PeopleSoft in July 2001. In addition, certain application fees, fixed assets, uncleared collections, investments and bank reconciliations did not show the name of the preparer and reviewer and/or the date they were prepared and reviewed.

SAM §8193 states that two monthly reconciliations are required for revolving fund transactions, one between the revolving fund and the general checking account, and the other between the revolving fund resources and the amount of cash advanced.

SAM §7908 requires all reconciliations to show the name of the preparer and reviewer, including the date the reconciliation was prepared and reviewed.

The director of fiscal services stated that revolving fund reconciliations had not been completed since the campus conversion to PeopleSoft because campus staff have been working on processes affected by the conversion that are prerequisites for performing effective revolving fund reconciliations. She further stated that the campus will resume performing the required revolving fund reconciliations when these prerequisite processes are adequately addressed. The assistant director of financial reports indicated his belief that the reconciliation procedures in place were adequate, but future reconciliations would comply with the signature and dating requirements.

Not completing reconciliations in a timely and complete manner compromises accountability and increases the risk that errors and irregularities will not be detected.

Recommendation 12

We recommend that the campus strengthen procedures to ensure that:

- a. Revolving fund reconciliations are performed monthly.
- b. All reconciliations include the names of the preparer and reviewer and the dates prepared and reviewed.

Campus Response

- a. We concur. The campus has completed development of a revolving fund reconciliation tool utilizing PeopleSoft query, and the reconciliation is being performed monthly for the items issued and cleared through the revolving fund in the preceding month.
- b. We concur. The university has instituted procedures to include preparer and reviewer signatures on all reconciliations.

Anticipated Completion Date: Complete.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Warren J. Baker	President
Karen Aguilar	Accounting Technician, Accounts Receivable
Douglas Allen	Equipment Technician III, Civil and Environmental Engineering
Kathy Anderson	Analyst/Programmer, Administration and Finance Division (AFD) Technology Services
Cheryl Andrus	Administrative Support Assistant, University Police
Michael Beaubien	Equipment Maintenance Technician, University Police
Olga Berdial	Student Assistant, Property
Harvey Blatter	Accountant
Laurie Borello	Operations Analyst, AFD Technology Services
Carol Clifford	Assistant Director, Payroll Services
Scott Cooke	Assistant Director, Financial Reports
Marlene Cramer	Business Services Coordinator
Jody Fisher	Accounting Technician
Lana Fleming	Information Center Coordinator, University Police
Marlene Gibbons	Accounting Technician
Janis Grieb	Student Accounts Manager
Judith Holloway	Accounting Technician, Student Accounts
Carol Johnston	Accounts Payable Manager
Betty Kroeze	Head of Support Services, Health Services, Student Affairs Division
Lorlie Leetham	Director of Fiscal Services
Frank Limon	Warehouse Supervisor, Shipping and Receiving
Dario Luis	Accountant, Extended University Programs and Services
Johanna Madjedi	Director, Communications and Computing Services
Valerie Maijala	Administrative Support Coordinator, Contracts and Procurement Services
Barbara Martin	Accounting Technician
David Mason	Manager, AFD Network and Technology Services
Barbara A. Melvin	Interim Director, Human Resources
Rachel Mendoza	Accounting Technician, Student Accounts
Fred Mills	Communications and Records Supervisor, Public Safety Services
Terri Mills	Administrative Assistant, University Police
Kimberly Perez	Accountant
Rick Ramirez	Associate Vice President for Finance
Joan Regulski	Accounting Technician
Nancy Reynolds	Assistant Director, Fiscal Services
Matthew Roberts	Director, Contract and Procurement Services
David Ross	Director, Application and Information Management
Giglia Sherman	Operations Analyst, AFD Technology Services
Patricia-Ann Stoneman	Director, Extended University Programs and Services
Vicki Stover	Associate Vice President for Administration
Fred Strasser	Supervising Property Clerk
John Sullivan	Accounting Technician, Travel Coordinator
Marilyn Tackitt	Administrative Support Assistant, University Police

APPENDIX A

Velma Tiberti	Accounting Technician, Accounts Payable
Patricia Vargas	Cashier, Health Services
Richard Walls	Coordinator, Information Technology Services
Lee Whitmer	Supervising Cashier
George Yelland	Director, AFD Technology Services

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.

CAL POLY

California Polytechnic State University
San Luis Obispo, CA 93407

Administration & Finance Division
(805) 756-2171 • Fax (805) 756-7560

RECEIVED
UNIVERSITY AUDITOR

NOV 12 2002

THE CALIFORNIA STATE
UNIVERSITY

November 8, 2002

Mr. Larry Mandel
University Auditor
Office of the University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802-4210

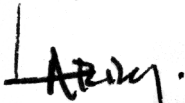
RE: Audit Report Number 02-04, *FISMA*, at California Polytechnic State University,
San Luis Obispo

Dear Mr. Mandel:

As requested in your letter of October 10, 2002, attached is the campus response to recommendations of Audit Report Number 02-04, *FISMA*. It is anticipated that documentation supporting audit findings that are specified as complete will be forwarded to you within the next few weeks.

If you have questions regarding this document, please contact Vicki Stover, Associate Vice President for Administration, at 805-756-2171 or vstover@calpoly.edu

Sincerely,



Lawrence R. Kelley
Vice President for Administration & Finance

cc: w/o attachments
W. Baker
V. Stover
R. Ramirez
L. Leetham
G. Yelland
M. Roberts
J. Hanley
J. Madjedi

**CALIFORNIA POLYTECHNIC STATE UNIVERSITY,
SAN LUIS OBISPO**

**FISMA
AUDIT REPORT NO. 02-04**

CASH RECEIPTS

Recommendation 1

We recommend that the campus:

- a. Establish procedures to utilize transfer receipts when transferring funds from university police to the cashier's office.
- b. Maintain a record of individuals who have access to the information booth safe and the date the combination was last changed.
- c. Strengthen procedures to ensure that all checks received in the university police reception area are endorsed by the end of the day.

Campus Response

- a. We concur. The University has instituted procedures for utilization of transfer receipts when transferring funds from University Police to the University Cashier's office.
- b. We concur. A record of individuals who have access to the information booth safe is being maintained and stored with the University Cashier's office.
- c. We concur. The University Police has strengthened procedures to ensure that checks are restrictively endorsed on a daily basis. Previous non-compliance in this area was found to be on an isolated basis and additional enforcement of the existing procedures should ensure compliance.

Anticipated Completion Date: Complete

PURCHASING

Recommendation 2

We recommend that the campus strengthen controls to ensure that original receipts or invoices are included in support of all procurement card purchases.

Campus Response

We concur. Emphasis will be placed on monthly submission requirements during training of cardholders. Additionally, the Approving Officials are being reminded that itemized invoices are required with each submission.

Anticipated Completion Date: Complete

REVOLVING FUND**Recommendation 3**

We recommend that the campus strengthen procedures to count petty cash and change funds in accordance with the prescribed schedule and obtain Department of Finance approval for the event parking fund.

Campus Response

We concur. The University has strengthened procedures to ensure that petty cash and change fund counts are performed in a timely manner in compliance with SAM provisions. University Cashiering personnel are performing the counts themselves to ensure the timely occurrence of counts in several of the areas. The three event parking change funds are now being maintained as completely separate change funds of \$200 each and are being counted and handled as such.

Anticipated Completion Date: Complete

PAYROLL/PERSONNEL**Recommendation 4**

We recommend that the campus strengthen separation procedures to ensure that separation forms are completed for all separated employees and revise the employee separation form to assure the settlement of any salary advances.

Campus Response

We concur. The University has instituted procedures to include review and settlement of salary advances as part of the separation form and procedures. Responsibility for monitoring completion of employee separation procedures has been assigned to that office responsible for completion of other steps in the separation process for certain groups of employees.

Anticipated Completion Date: Complete

FIXED ASSETS

PHYSICAL INVENTORY

Recommendation 5

We recommend that the campus complete the physical inventories of the computer center and facility services and report the results to management.

Campus Response

We concur. The facility services inventory has been completed and the computer center inventory has been divided up into smaller, more manageable units to allow for completion of the inventories within the required timeframes.

Anticipated Completion Date: December 31, 2002

FISCAL INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

Recommendation 6

We recommend that the campus:

- a. Enhance the IT DRP by adding detailed procedures for all sections outlined in SAM, develop campus business continuity plans to sustain operations during an extended outage of data processing services, and add an assumptions list that should be shared with the business users to enhance their understanding of what services will and will not be restored as part of the IT recovery plan. The assumptions list should also reflect the status of data files at the time of restoration.
- b. Conduct a business impact assessment to determine the maximum length of time that the departments could operate without data processing services, and identify the equipment and information that would be needed to sustain operations during an outage of data processing services.
- c. Develop written manual operating and recovery procedures for business units to assist operations during an extended outage of data processing services, such as manual recovery of up to one week of lost data, and procedures for entering data collected manually during a prolonged system outage.

Campus Response

a. & b. SAM §4843 recommends the following elements in the operational recovery planning process. Responses to these elements are noted in italics.

The operational recovery planning process provides necessary preparation to design and document a sufficient set of procedures to assure continued agency operations in the event of a disaster or any other event resulting in unplanned discontinuation of IT systems operations. Each agency's process should include the following elements and culminate with the documentation of results in the form of an Operational Recovery Plan:

- 1 Establishment of an Operational Recovery Planning Team which will be responsible for the detailed technical analysis and planning functions that are fundamental to an operational plan;

Included in Disaster Recovery Plan—Section 4D, Recovery Team Concept provided on 9/17/02.

2. Development of an understanding of the agency's mission, including the organizational, managerial, and technical environments within which an effective Operational Recovery Plan must work;

Included in Disaster Recovery Plan—Section 4A, Introduction provided on 9/17/02.

3. Re-assessment of the agency's identification of the most probable types of disaster occurrences and the cost effective protective measures to be implemented, that were identified as a result of the risk management process. See SAM §4842 through 4842.21 for risk management policies;

Included in Disaster Recovery Plan—Section 4A, Introduction; 4C, Risk Assessment Summary provided on 9/17/02.

4. Assessment of the resource requirements (equipment, communications, data, software, personnel and time) required for the agency's critical applications identified through the risk management process;

Included in Disaster Recovery Plan—Section 4E, Business Impact Analysis, and 4F, Risk Assessment provided on 9/17/02.

5. Identification and evaluation of alternative recovery strategies;

A proposal to Cal Poly Management Staff in Fall 2001 recommended having on-site trailers as an Alternate Site. Recommendation approved. Sites identified. In process of determining costs for umbilical power and network connectivity and selecting trailer provider.

Anticipated Completion Date: June 30, 2003.

6. Preparation of a cost benefit analysis for each alternative;

See response to #5.

7. Selection of the alternative that best responds to the agency's requirements for disaster recovery;

See response to #5.

8. Determination of specific recovery procedures and the time frame for their execution;

See response to #4 and #5.

9. Identification of individuals or teams within the agency that will be responsible for managing and implementing specific recovery procedures; and

See response to #1.

10. Documentation of the results of the planning process in the form of an Operational Recovery Plan, as specified in SAM §4843.1 and §4845.

Provided to auditors on 9/17/02.

- c. We concur. There is a need for written procedures to assist operations during an extended outage of data processing services. Given that our data processing center backs up our data on a daily basis and creates an offsite copy, the most likely scenarios is the loss of a day's worth of activity or an extended outage of the center.

Anticipated Completion Date: March 31, 2003

PROGRAM CHANGE CONTROL

Recommendation 7

We recommend that the campus restrict all programmers from update access to production copies of programs and data or establish a detective control to identify programs that have been changed and require management to review such changes on a regular basis, as well as require specific written authorization from management for data access.

Campus Response

The ITS department currently operates without a formal librarian role and/or librarian software application which would be needed to fully implement and meet the requirements of this recommendation. We will pursue the following:

1. Implement an automated logging process to identify programmers who compiled jobs within the production environment; and

2. Review the logs on a regular basis to identify inappropriate activity.
3. Publish the current procedures for providing data access.

Anticipated Completion Date: December 31, 2002

MAINFRAME SECURITY

Recommendation 8

We recommend that the campus:

- a. Change the aforementioned RACF settings regarding tape data set protection and the RVAR Y command to provide stronger security.
- b. Review the use of special privileges and ensure that they are assigned to only those individuals that require such access to perform their normal job duties.

Change the universal access code setting to NONE for sensitive SYS1 libraries in order to reduce the risk of unauthorized modification or disclosure.

Campus Response

Tape DSN—Cal Poly will consult with CSU-Hayward since this is a global RACF change that affects both campuses.

RACF SPECIAL—A review of accounts with RACF SPECIAL was conducted with these findings:

- Cal Poly and CSU-Hayward share the same mainframe environment and each campus manages security for their own resources, requiring RACF administrators at each campus with “department” SPECIAL
- Staff members at the Cal Poly Help Desk have limited RACF capabilities allowing them to change Cal Poly user passwords.

Default RVAR Y password—The IBM default RVAR Y password has been changed as recommended.

One account with SPECIAL that is revoked but not deleted is IBMUSER. That account must remain on the system to support IBM upgrades. Two other accounts were requested by the auditors during the last FISMA audit and have been deleted.

Anticipated Completion Date:

Tape DSN security in WARN mode – December 1, 2002

Tape DSN security in FAIL mode – January 1, 2003

PEOPLESOFT SECURITY

Recommendation 9

We recommend that the campus address the deficiencies in PeopleSoft password security either by implementing the PentaSafe software or through enhancing security through other means.

Campus Response

Cal Poly expects to implement PeopleSoft Release 8.0 for Human Resources by July 1, 2003. PeopleSoft 8.X implementation for Financials is planned for February 2004. Enhanced security for Financials 7.5 is currently under review by CMS Central staff and we will implement their suggestions after they are published. Anticipated completion date: August 2003 (after completion of year-end close and contingent on development by CMS Central staff)

USER ACCOUNT REMOVAL

Recommendation 10

We recommend that the campus ensure that the process for assigning and removing IDs is consistent across all computing platforms and application systems.

Campus Response

We concur. In order to ensure that the process for assigning and removing ITS is consistent across all computing platforms and application systems, ITS is in the process of building a middleware infrastructure that will support central authentication services. This is in coordination with the statewide Middleware Initiative for the CSU.

One of the first phases of this project is to create an identity reconciliation system capable of storing necessary attributes. Once completed, ITS will encourage application administrators to utilize central authentication services against the enterprise directory.

While this will allow the pursuance of central authentication, moving the campus applications into this infrastructure will be an on-going process.

Anticipated Completion Date: December 31, 2002

VENDOR ACCESS TO CASHNET

Recommendation 11

We recommend that the campus:

Restrict vendors from directly 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. Develop a method to prohibit access to credit card information by vendor personnel.

Campus Response

We concur.

Vendor Access will be controlled via AIX account management. A procedure is being developed to enable and disable the support account. Vendor access to the system will be by request only. Access will be disabled by Cal Poly personnel after a support event.

Anticipated Completion Date: December 31, 2002

Effective with release 5.38 of the Cashnet software the credit card information will be encrypted. Cal Poly plans to implement this release in December of 2002.

Anticipated Completion Date: December 31, 2002

RECONCILIATIONS

Recommendation 12

We recommend that the campus strengthen procedures to ensure that:

- a. Revolving fund reconciliations are performed monthly.
- b. All reconciliations include the names of the preparer and reviewer and the dates prepared and reviewed.

Campus Response

- a. We concur. The campus has completed development of a revolving fund reconciliation tool utilizing PeopleSoft query and the reconciliation is being performed monthly for the items issued and cleared through the revolving fund in the preceding month.
- b. We concur. The University has instituted procedures to include preparer and reviewer signatures on all reconciliations.

Anticipated Completion Date: Complete

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

January 10, 2003

CHANNEL ISLANDS

CHICO

MEMORANDUM

DOMINGUEZ HILLS

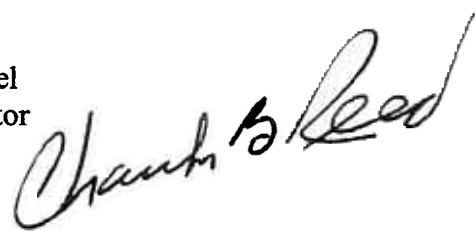
FRESNO

TO: Mr. Larry Mandel
University Auditor

FULLERTON

HAYWARD

FROM: Charles B. Reed
Chancellor



HUMBOLDT

SUBJECT: Draft Final Report Number 02-04 on *FISMA*,
California Polytechnic State University, San Luis Obispo

LONG BEACH

LOS ANGELES

MARITIME ACADEMY

In response to your memorandum of January 10, 2003, I accept the response as submitted with the draft final report on *FISMA*, California Polytechnic State University, San Luis Obispo.

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/amd

SACRAMENTO

Enclosure

SAN BERNARDINO

SAN DIEGO

cc: Dr. Warren J. Baker, President

SAN FRANCISCO

SAN JOSE

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS