

FISMA

OFFICE OF THE CHANCELLOR

Report Number 01-07

November 29, 2001

Members, Committee on Audit

Shailesh J. Mehta, Chair
Stanley T. Wang, Vice Chair
Daniel N. Cartwright Murray L. Galinson
Harold Goldwhite Ricardo F. Icaza
Frederick W. Pierce, IV

Staff

University Auditor: Larry Mandel
Senior Director: Janice Mirza
Audit Manager: Jim Usher
IS Audit Manager: Greg Dove

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 MANAGEMENT RESPONSES

Cash Receipts	7
Revolving Fund.....	7
Unauthorized Fund.....	7
Infrequent Fund Counts	8
Purchasing	9
Separation of Duties	9
Procard Statement Approval	9
Cash Disbursements/Accounts Payable.....	10
Disbursement Authorization	10
Check Cancellation.....	11
Payroll/Personnel	11
Authorization Signatures	11
Overtime Approval.....	12
Fiscal Information Technology	12
Disaster Recovery Plan.....	12
Mainframe User Account Settings and Removal.....	13
Program Change Control	14
Mainframe Security	15
UNIX and Oracle User Accounts	16
Trust Funds	17

APPENDICES

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

ABBREVIATIONS

BMS	Business Management Systems
CITS	Chancellor's Office Information Technology Services
CMS	Common Management System
CPDC	Capital Planning, Design and Construction
CSU	California State University
DOF	Department of Finance
EO	Executive Order
FISMA	Financial Integrity and State Manager's Accountability Act
FRS	Financial Records System
IT	Information Technology
OSG	Operating Systems Group
SAM	State Administrative Manual
SCO	State Controller's Office
UAC	Universal Access Code

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 years 1999-2000 and 2000-01 were the primary periods reviewed. In certain instances, we were concerned with representations of the most current data—in such cases, the test period was through June 2001. 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 Office of the Chancellor from May 14, 2001, through July 13, 2001, and made a study and evaluation of the accounting and administrative control in effect as of July 13, 2001. 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.

Management in the Office of the Chancellor is responsible for establishing and maintaining adequate internal control. This responsibility, in accordance with Government Code §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 Office of the Chancellor did not maintain adequate control over the following areas: revolving funds, purchasing, disbursements, and fiscal information technology.

These conditions, along with other weaknesses, are described in the executive summary and in the body of the report.

In our opinion, except for the effect of the weaknesses described above, the chancellor's office accounting and administrative controls in effect as of March 29, 2001, 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 [7]

There was no procedure to periodically request local banks to search for unauthorized bank accounts that use the campus name, address, and federal identification number. Establishing a process to periodically search for unauthorized bank accounts reduces the risk of liability associated with improper bank accounts.

REVOLVING FUND [7]

UNAUTHORIZED FUND [7]

A \$600 petty cash fund in the parking and transportation office at California State University (CSU), Channel Islands that grew to \$1,000 was established without appropriate authorization. Fund authorization by the Department of Finance strengthens internal controls and compliance with state policy.

INFREQUENT FUND COUNTS [8]

Independent cash counts of certain change funds did not always occur with the required frequency. Counts conducted at prescribed frequencies ensure adequate internal control over cash and reduce the risk of loss.

PURCHASING [9]

SEPARATION OF DUTIES [9]

Buyers and accounts payable technicians were authorized to record goods and services as received. Separation of these duties reduces the risk of erroneous payments for goods and services not received.

PROCARD STATEMENT APPROVAL [9]

Capital Planning, Design and Construction (CPDC) monthly procurement card statements were not approved by the cardholder's supervisor. Reviews of statements by an appropriate approving official reduce the risk of procurement card misuse.

CASH DISBURSEMENTS/ACCOUNTS PAYABLE [10]

DISBURSEMENT AUTHORIZATION [10]

Unauthorized persons were approving invoices for payment. Proper payment authorizations reduce the risk of improper disbursements.

CHECK CANCELLATION [11]

Checks older than one year were not being cancelled. Cancelling or remitting long-outstanding checks stops reversion to the General Fund, eases the reconciliation effort, and decreases the risk of inappropriate acts.

PAYROLL/PERSONNEL [11]

AUTHORIZATION SIGNATURES [11]

Payroll/personnel signature authorizations were not updated on a timely basis. Current signature authorizations improve controls over payroll transactions and decrease the risk of inappropriate payroll expenditures.

OVERTIME APPROVAL [12]

Overtime for the last couple of days in a month was not certified after-the-fact in writing to document that the hours were actually worked. Strengthening overtime approval reduces the risk of payroll irregularities.

FISCAL INFORMATION TECHNOLOGY [12]

DISASTER RECOVERY PLAN [12]

There was no written information technology (IT) disaster recovery plan for either the UNIX operations at West Ed or the mainframe system supported by CSU Fresno, and there were no manual departmental operating and recovery procedures for business units. A detailed IT disaster recovery plan and corresponding business continuation procedures would assist the chancellor's office in restoring computer operations within a reasonable time frame and the continuation of normal business operations.

MAINFRAME USER ACCOUNT SETTINGS AND REMOVAL [13]

Security administration over logon accounts did not ensure that system access was adequately restricted. Adequate controls over logon accounts improve system security and reduce the possibility of inadvertent access.

PROGRAM CHANGE CONTROL [14]

Policies and procedures over program change management were not formally documented, and existing practices did not prevent all persons with programming responsibilities from making unauthorized changes to production. Restricting the capability of programmers to make changes directly to production copies of programs improves management assurances that changes are authorized.

MAINFRAME SECURITY [15]

Some mainframe security (RACF) parameters were not set to provide effective protection, and many sensitive libraries were not sufficiently protected. Improving controls over user account settings and account removal reduces the risk of granting inappropriate access and improves password confidentiality.

UNIX AND ORACLE USER ACCOUNTS [16]

Passwords for accounts on the UNIX operating system and the Oracle database system were not set to expire after a predetermined amount of time, and IDs assigned to campuses were not restricted to a single user. Proper password control and enforcement improve password confidentiality and logon accountability.

TRUST FUNDS [17]

Trust fund agreements were not always complete and approved. Adequate administration of trust agreements decreases the risk of inappropriate expenditures.

OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

CASH RECEIPTS

There was no procedure to periodically request local banks to search for unauthorized bank accounts that use the campus name, address, and federal identification number.

Government Code §13401(b)(3) states that all levels of management of state agencies must be involved in assessing and strengthening the systems of internal accounting and administrative control to minimize fraud, errors, abuse, and waste of government funds.

The director of accounting stated that bank surveys are not a worthwhile exercise for the chancellor's office environment.

Not establishing a process to periodically search for unauthorized bank accounts increases the risk of the campus being associated with improper bank accounts.

Recommendation 1

We recommend that the Office of the Chancellor establish and implement procedures to periodically request local banks to search for unauthorized bank accounts that use the university's name, address, and federal identification number.

Management Response

We concur. The described requests have been sent to local banks. The decision to continue the procedure will be based on the level of responses received from the banks.

REVOLVING FUND

UNAUTHORIZED FUND

A \$600 petty cash fund in the parking and transportation office at California State University (CSU), Channel Islands that grew to \$1,000 was established without appropriate authorization.

The Office of the Chancellor had been providing fiscal services to CSU Channel Islands since its inception. These services were transferred to CSU Northridge effective July 1, 2001.

State Administrative Manual (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 (DOF).

The associate vice president for administrative services at CSU Channel Islands stated that he had assumed the fund was authorized.

The absence of DOF authorization compromises internal controls and results in noncompliance with state policy.

Recommendation 2

We recommend that the Office of the Chancellor apprise CSU Channel Islands and CSU Northridge of the need to obtain DOF approval for the CSU Channel Islands parking and transportation office petty cash fund.

Management Response

We concur. The chancellor's office will notify the campuses of the requirements to obtain DOF approval for petty cash funds by March 1, 2002.

INFREQUENT FUND COUNTS

Independent cash counts of certain change funds did not always occur with the required frequency.

Four of six funds were not counted frequently enough. The missing counts included:

- ▶ The ten months of July, August, September, November, December, January, February, March, April, and June for the \$600 fund in the parking and transportation office at CSU Channel Islands.
- ▶ The second quarter for the \$500 in the accounting office.
- ▶ The second and third quarters for the \$300 in the president's office at CSU Channel Islands.
- ▶ The second and third quarters for the \$250 in the Sacramento Office of Governmental Affairs.

SAM §8111.2 requires a change or petty cash count in accordance with the following frequency: (a) \$200.00 or less on an annual basis; (b) \$200.01 to \$500.00 on a quarterly basis; (c) \$500.01 to \$2,500.00 on a monthly basis; (d) over \$2,500.00 on a monthly basis, if not prescribed more frequently by the Fiscal Systems and Consulting Unit, Department of Finance.

The accounts payable manager stated that the counts were infrequent and not well documented because the fund custodians were not under their supervision and not physically located within the chancellor's office.

Not conducting independent cash counts at prescribed frequencies compromises internal controls and increases the risk of loss.

Recommendation 3

We recommend that the Office of the Chancellor implement procedures to ensure that cash funds are counted at prescribed frequency intervals.

Management Response

We concur. The Office of the Chancellor will implement procedures that ensure cash funds are counted at prescribed frequency intervals. The procedures will include identifying those positions responsible for counting the funds as well as reviewing the counts. The procedure will be implemented by March 1, 2002.

PURCHASING

SEPARATION OF DUTIES

Buyers and accounts payable technicians were authorized to record goods and services as received.

SAM §20050 states that the elements of an adequate system of internal accounting and administrative controls include a system of authorization and record-keeping procedures adequate to provide effective control over assets, liabilities, revenues, and expenditures.

The director of Contract Services and Procurement and the accounts payable manager stated that their access was a backup in case receiving was unavailable.

Combining these duties increases the risk of erroneous payments for goods and services not received.

The ability of buyers and accounts payable technicians to receive goods and services was restricted during the course of the audit. It is management's intention that this restriction will be permanent.

PROCARD STATEMENT APPROVAL

Capital Planning, Design and Construction (CPDC) monthly procurement card statements were not approved by the cardholder's supervisor.

All CPDC monthly procurement card statements were approved by one person with no reporting relationship to the cardholders. This approving official reports to a section chief as do many of the CPDC cardholders.

Executive Order (EO) No. 760, *Procurement Cards*, dated October 16, 2000, states that an approving official cannot be a peer or subordinate.

The director of accounting stated that a review of CPDC procurement card authorization was underway.

Procurement card statement review by an inappropriate approving official increases the risk of card misuse.

Recommendation 4

We recommend that the Office of the Chancellor strengthen the procurement card process to ensure that designated approving officials are not cardholders' peers or subordinates.

Management Response

We concur. A review of authorizations of procurement cards issued to CPDC was performed. As a result, the cards were reissued to avoid approval by the cardholders' subordinate or peer.

CASH DISBURSEMENTS/ACCOUNTS PAYABLE

DISBURSEMENT AUTHORIZATION

Unauthorized persons were approving invoices for payment.

In the chancellor's office Financial Records System (FRS) application, individuals authorized to approve disbursements on accounts were identified on certain FRS screens. Our review of 25 transactions disclosed 19 (76%) transactions where the person approving the invoice for payment was different than the person authorized to sign on the account.

SAM §20050 states that the elements of an adequate system of internal accounting and administrative controls include a system of authorization and record-keeping procedures adequate to provide effective control over assets, liabilities, revenues, and expenditures.

The director of accounting stated that the FRS system does not adequately capture delegations of authority.

Inadequate controls over payment authorizations increase the risk of improper disbursements.

Recommendation 5

We recommend that the Office of the Chancellor review disbursement authorization practices to ensure that transactions are only approved by authorized individuals.

Management Response

We concur. The chancellor's office will adopt policy and practices to ensure that transactions will be approved only by authorized individuals. The policy will be issued by March 15, 2002.

CHECK CANCELLATION

Checks older than one year were not being cancelled.

Our review of the bank reconciliation, dated June 30, 2001, disclosed 51 checks older than one year.

SAM §8042 indicates that revolving fund and agency checks issued on or after January 1, 1998, have a one-year period of negotiability.

The general accounting manager stated that the check review process was delayed because of employee turnover.

Not cancelling or remitting long-outstanding checks and warrants timely could result in reversion to the General Fund, require additional effort to review outstanding checks and warrants during the reconciliation process, and increase the risk of inappropriate acts.

Recommendation 6

We recommend that the Office of the Chancellor establish procedures to promptly cancel checks older than one year.

Management Response

We concur. The chancellor's office will adopt policy to cancel checks older than one year. The policy will be issued by March 15, 2002.

PAYROLL/PERSONNEL

AUTHORIZATION SIGNATURES

Payroll/personnel signature authorizations were not updated on a timely basis.

On July 10, 2001, the chancellor's office submitted new signature documents to the State Controller's Office (SCO) to process nine changes, which included five deletions and four additions to personnel authorized to sign payroll/personnel transactions. Some of the deletions were due to retirements prior to July 1999.

The state's *Payroll Procedures Manual* requires agencies to file payroll/personnel authorization signatures with the SCO.

The manager of benefits stated that the signatures were not updated because of employee turnover.

Outdated signature authorizations weaken controls over payroll transactions and increase the risk of inappropriate payroll expenditures.

The signature authorizations were updated during the audit.

OVERTIME APPROVAL

Overtime for the last couple of days in a month was not certified after-the-fact in writing to document that the hours were actually worked.

SAM §8540 indicates that care should be exercised in recording the overtime hours on the monthly attendance reports and overtime records of the employing state agency. The state's Std. 662 form provides space for certification that hours have actually been worked.

The manager of benefits stated that the process is designed to expedite overtime payments according to the payroll cutoffs established by the state.

Certifying end-of-the-month overtime only on a verbal basis after it has been worked increases the risk of payroll irregularities.

Recommendation 7

We recommend that the Office of the Chancellor establish procedures to ensure that end-of-the-month overtime is certified in writing after it has been worked.

Management Response

We concur. The chancellor's office Payroll Department will require that department managers initial any overtime worked after the form is submitted.

FISCAL INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

There was no written information technology (IT) disaster recovery plan for either the UNIX operations at West Ed or the mainframe system supported by CSU Fresno, and there were no manual departmental operating and recovery procedures for business units.

The IT department had taken initial steps to ensure that data would be available for recovery; however, without a recovery plan, there was no assurance that data processing services could be recovered in a timely manner. In addition, there were no manual departmental operating and recovery procedures for business units during an extended outage of data processing services. Since the daily backup tapes

remained on-site, the business units needed to determine if a potential loss of up to one week's worth of data could be re-created and the impact to their business operations.

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 the agency's plans for resuming operation following a disaster affecting those applications.

EO No. 696, *Implementation of the CSU 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 senior director of the Chancellor's Office Information Technology Services (CITS) stated that high-level plans were in place to acquire the necessary hardware for the UNIX operation backup, and data recovery procedures were documented; however, comprehensive, detailed recovery policies and procedures had not been developed.

Without a detailed IT disaster recovery plan and corresponding business continuation procedures, the chancellor's office may not be able to restore computer operations within a reasonable time frame, which could severely impact the ability to conduct normal business operations.

Recommendation 8

We recommend that the Office of the Chancellor develop an IT disaster recovery plan for the financial and data warehouse systems as well as manual operating and recovery procedures for use by the business units in the event of an extended outage of data processing services.

Management Response

We concur. The chancellor's office will work with CSU Fresno (where the MVS operations are outsourced) on plans to address recovery of the financial systems and data on the MVS. Such plans will be developed by April 30, 2002. The chancellor's office will also complete recovery plans and procedures for the systems and data at the WestEd facility by April 30, 2002.

MAINFRAME USER ACCOUNT SETTINGS AND REMOVAL

Security administration over logon accounts did not ensure that system access was adequately restricted.

Specifically, we noted:

- ▶ Expired IDs for the mainframe computer had not been deleted from the system.
- ▶ Inactive accounts were not being revoked.

- ▶ Only three generations of password history were being maintained.
- ▶ Ten unsuccessful access attempts were allowed before an account was revoked.

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 senior director of CITS stated that the procedures for maintaining account settings had been in place for several years and had not been recently examined, as the long-term plan is to implement the Common Management System (CMS) software and be in production by October 1, 2002.

Inadequate controls over logon accounts increase the risk of personnel being granted inappropriate access if a revoked ID is reissued, unauthorized access to systems through inactive accounts, password confidentiality being compromised, and unauthorized access to systems through multiple logon attempts.

Recommendation 9

We recommend that the Office of the Chancellor delete all IDs that are no longer used, turn on the setting to automatically revoke accounts that have not been accessed for an extended period of time, change the password history setting to record at least ten successive passwords, and lower the limit for unsuccessful access attempts to three.

Management Response

We concur. CITS is working closely with CSU Fresno Operating Systems Group (OSG) to review and delete userids that are no longer used and will implement the other recommendations for access control by January 31, 2002.

PROGRAM CHANGE CONTROL

Policies and procedures over program change management were not formally documented, and existing practices did not prevent all persons with programming responsibilities from making unauthorized changes to production.

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 senior director of CITS 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 programs, management cannot be assured that all changes made are authorized and, consequently, that internal controls are not compromised.

Recommendation 10

We recommend that if all programmers cannot effectively be restricted from update access to production copies of programs, then a detective control reflecting programs that have been changed should be produced and reviewed by management on a regular basis.

Management Response

We concur. The Business Management Systems (BMS) group has been contracted by CITS to maintain the Systemwide and Chancellor's Office Local-Mod libraries of program sources and executable object for the Financial Reporting System (FRS) since August 2001. CITS will work with BMS to establish regular change control reports for review by CITS management by April 30, 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:

- ▶ Protect All, which places newly created data sets under RACF protection, was not in effect.
- ▶ Tape DSN, which enables protection of data sets stored on tape, was not in effect.
- ▶ Security over the job entry subsystem and the batch job handler was not active, which could permit the submission of unauthorized jobs.
- ▶ RACF special privileges had been granted to individuals that did not need such access to perform their job responsibilities.
- ▶ Many RACF authorized libraries were not RACF protected, which could be exploited to gain unauthorized access to system resources.
- ▶ Systemwide read access to libraries whose names begin with high level "SYS1" 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 senior director of CITS stated that the procedures for maintaining parameter settings had been in place for several years and had not been recently examined, as the long-term plan is to implement the CMS software and to be in production by October 1, 2002.

Since the 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 11

We recommend that:

- a. The aforementioned RACF settings regarding protect All, tape data set protection, batch and online job submission, and use of special privileges be changed to provide stronger security.
- b. The universal access code (UAC) setting be changed to READ or NONE for RACF and authorized SYS1 libraries in order to reduce the risk of unauthorized modifications or disclosure.

Management Response

We concur. CITS will work with BMS and CSU Fresno to implement the above recommendations. The new procedures and settings will be completed by January 31, 2002.

UNIX AND ORACLE USER ACCOUNTS

Passwords for accounts on the UNIX operating system and the Oracle database system were not set to expire after a predetermined amount of time, and IDs assigned to campuses were not restricted to a single user.

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 senior director of CITS stated that the procedures for maintaining parameter settings had been in place for several years and had not been recently examined and that campus users had not been restricted to one ID per user. The Office of the Chancellor allocates one ID per application (Accounting, Budget, Auxiliaries) for reporting FIRMS data and it is the campus' responsibility to protect access and use of the IDs. The vice presidents were required to sign off on the designated user of each ID.

Not setting passwords to expire increases the likelihood that password confidentiality could become compromised, and not enforcing the individual use of logon accounts does not support appropriate accountability.

Recommendation 12

We recommend that UNIX and Oracle passwords be set to automatically expire within a reasonable time frame and that campus users be required to follow the established policies and procedures for accessing Office of the Chancellor systems.

Management Response

We concur. CITS will implement the user password expiration features as recommended on at least one of the current servers (Sage) by January 31, 2002, and the features will be implemented and enforced on all new UNIX systems as they are installed.

TRUST FUNDS

Trust fund agreements were not always complete and approved.

Our review of ten trust agreements disclosed three instances (758894, 759390, and 759680) where the agreements did not contain the signatures of those authorized to sign on the account and had not been approved.

SAM §19440.1 states that each trust account established shall be supported by documentation as to the type of trust, donor, or source of trust moneys, purpose of the trust, time constraints, persons authorized to withdraw or expend funds, specimen signatures, reporting requirements, instructions for closing the account, disposition of any unexpended balance, and restrictions on the use of moneys for administrative or overhead costs.

The director of accounting indicated that improper prioritization of workload contributed to the incomplete agreements.

Inadequate trust fund administration increases the risk of inappropriate expenditures.

Recommendation 13

We recommend that the Office of the Chancellor strengthen procedures over trust fund administration to ensure that all trust projects have complete agreements on file.

Management Response

We concur. Annually, the Office of the Chancellor will review all trust accounts to ensure a completed agreement is on file for all active trust accounts.

APPENDIX A: PERSONNEL CONTACTED

OFFICE OF THE CHANCELLOR

<u>Name</u>	<u>Title</u>
Richard West	Executive Vice Chancellor and Chief Financial Officer
Jackie Bowman-Childers	Payroll Technician
Addison Ching	Director, Information Dissemination and Access
Shahenaz Chruiwala	Manager, Cash and Investments
Anita Corliss	Manager, Benefits
Ted Dang	Payroll Technician
Pat Dayneko	Director, Contract Services and Procurement
Jan Earl	Financial Systems Coordinator
Lisa Gibbons	Accountant
Bruce Gibson	Senior Director, Personnel/Payroll
Ellyce Gordon	Property Clerk
Cheryl Kwiatkowski	Senior Director, Chancellor's Office Information Technology Services
Diana Lam-Brandt	Accounts Receivable Accountant
Melanio Lorenzo	Lottery/Trust Accountant
Linda Masterton	Lead Buyer
Bill Musselman	Director of Accounting
Mark Osborne	Tax Manager
Art Phillips	Director, Corporate Information Systems
Mary Ann Rodriguez	Director of Administration
Lenore Rozner	Assistant Vice Chancellor, Business Planning and Information Systems
Cynthia St. Amant	Accounting Technician
Ruth Stipp	General Accounting Manager
Daphne Sumner	Accounts Payable Manager

CSU CHANNEL ISLANDS

<u>Name</u>	<u>Title</u>
Caroline Doll	Leasing Coordinator
Lashanor Doolittle	Coordinator, Business Services – Transportation and Parking Services
George Dutra	Associate Vice President, Facilities Development and Operations
Art Flores	Associate Vice President, Administrative Services
Leah Kirklin	Coordinator, Budget and Finance
Ray Porras	Director, Transportation and Parking 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.



THE CALIFORNIA STATE UNIVERSITY

BAKERSFIELD • CHANNEL ISLANDS • CHICO • DOMINGUEZ HILLS • FRESNO • FULLERTON • HAYWARD • HUMBOLDT
 LONG BEACH • LOS ANGELES • MARITIME ACADEMY • MONTEREY BAY • NORTHRIDGE • POMONA • SACRAMENTO
 SAN BERNARDINO • SAN DIEGO • SAN FRANCISCO • SAN JOSE • SAN LUIS OBISPO • SAN MARCOS • SONOMA • STANISLAUS

RICHARD P. WEST
 EXECUTIVE VICE CHANCELLOR AND
 CHIEF FINANCIAL OFFICER

MEMORANDUM

RECEIVED
 University Auditor

Date: January 9, 2002

JAN 09 2002

TO: Mr. Larry Mandel
 University Auditor

**The California State
 University**

FROM: Richard P. West
 Executive Vice Chancellor
 Chief Financial Officer

SUBJECT: FISMA Report Number 01-07

Attached is the Chancellor's Office response to the FISMA audit findings and recommendations. Our responses are based on a review of the controls identified by your staff as needing improvement. We believe our corrective plan will be sufficient to restore or upgrade critical controls.

We would like to thank your staff for the professionalism displayed during the course of the audit.

Mr. Larry Mandel
January 9, 2002
Page 2

OFFICE OF THE CHANCELLOR

**FISMA
AUDIT REPORT NO. 01-07**

CASH RECEIPTS

Recommendation 1

We recommend that the Office of the Chancellor establish and implement procedures to periodically request local banks to search for unauthorized bank accounts that use the university's name, address, and federal identification number.

Management Response

We concur. The described requests have been sent to local banks. The decision to continue the procedure will be based on the level of responses received from the banks.

REVOLVING FUND

UNAUTHORIZED FUND

Recommendation 2

We recommend that the Office of the Chancellor apprise CSU Channel Islands and CSU Northridge of the need to obtain DOF approval for the CSU Channel Islands parking and transportation office petty cash fund.

Management Response

We concur. The Chancellor's Office will notify the campuses of the requirements to obtain DOF approval for petty cash funds by March 1, 2002.

INFREQUENT FUND COUNTS

Recommendation 3

We recommend that the Office of the Chancellor implement procedures to ensure that cash funds are counted at prescribed frequency intervals.

Management Response

We concur. The Office of the Chancellor will implement procedures that ensure cash funds are counted at prescribed frequency intervals. The procedures will include identifying those positions

Mr. Larry Mandel
January 9, 2002
Page 3

responsible for counting the funds as well as reviewing the counts. The procedure will be implemented by March 1, 2002.

PURCHASING

PROCARD STATEMENT APPROVAL

Recommendation 4

We recommend that the Office of the Chancellor strengthen the procurement card process to ensure that designated approving officials are not cardholders' peers or subordinates.

Management Response

We concur. A review of authorizations of procurement cards issued to CPDC was performed. As a result, the cards were reissued to avoid approval by the cardholders' subordinate or peer.

CASH DISBURSEMENTS/ACCOUNTS PAYABLE

DISBURSEMENT AUTHORIZATION

Recommendation 5

We recommend that the Office of the Chancellor review disbursement authorization practices to ensure that transactions are only approved by authorized individuals.

Management Response

We concur. The Chancellor's Office will adopt policy and practices to ensure that transactions will be approved only by authorized individuals. The policy will be issued by March 15, 2002.

CHECK CANCELLATION

Recommendation 6

We recommend that the Office of the Chancellor establish procedures to promptly cancel checks older than one year.

Management Response

We concur. The Chancellor's Office will adopt policy to cancel check older than one year. The policy will be issued by March 15, 2002.

Mr. Larry Mandel
January 9, 2002
Page 4

PAYROLL/PERSONNEL

OVERTIME APPROVAL

Recommendation 7

We recommend that the Office of the Chancellor establish procedures to ensure that end-of-the-month overtime is certified in writing after it has been worked.

Management Response

We concur. The Chancellor's Office Payroll Department will require that department managers initial any overtime worked after the form is submitted.

FISCAL INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

Recommendation 8

We recommend that the Office of the Chancellor develop an IT disaster recovery plan for the financial and data warehouse systems as well as manual operating and recovery procedures for use by the business units in the event of an extended outage of data processing services.

Management Response

We concur. The Chancellor's Office will work with CSU Fresno (where the MVS operations are outsourced) on plans to address recovery of the Financial Systems and data on the MVS. Such plans will be developed by April 30, 2002. The Chancellor's Office will also complete recovery plans and procedures for the systems and data at the WestEd facility by April 30, 2002.

MAINFRAME USER ACCOUNT settings and REMOVAL

Recommendation 9

We recommend that the Office of the Chancellor delete all IDs that are no longer used, turn on the setting to automatically revoke accounts that have not been accessed for an extended period of time, change the password history setting to record at least ten successive passwords, and lower the limit for unsuccessful access attempts to three.

Management Response

Mr. Larry Mandel
January 9, 2002
Page 5

We concur. CITS is working closely with CSU, Fresno Operating Systems Group (OSG) to review and delete userids that are no longer used and will implement the other recommendations for access control by January 31, 2002.

PROGRAM CHANGE CONTROL

Recommendation 10

We recommend that if all programmers cannot effectively be restricted from update access to production copies of programs, then a detective control reflecting programs that have been changed should be produced and reviewed by management on a regular basis.

Management Response

We concur. The Business Management Systems (BMS) group has been contracted by CITS to maintain the Systemwide and Chancellor's Office Local-Mod libraries of program sources and executable object for the Financial Reporting System (FRS) since August, 2001. CITS will work with BMS to establish regular change control reports for review by CITS management by April 30, 2002.

MAINFRAME SECURITY

Recommendation 11

We recommend that:

- a. The aforementioned RACF settings regarding protect all, tape data set protection, batch and online job submission, and use of special privileges be changed to provide stronger security.
- b. The universal access code (UAC) setting be changed to READ or NONE for RACF and authorized SYS1 libraries in order to reduce the risk of unauthorized modifications or disclosure.

Management Response

We concur. CITS will work with BMS and CSU Fresno to implement the above recommendations. The new procedures and settings will be completed by January 31, 2002.

UNIX and oracle USER ACCOUNTS

Recommendation 12

We recommend that UNIX and Oracle passwords be set to automatically expire within a reasonable time frame and that campus users be required to follow the established policies and procedures for accessing Office of the Chancellor systems.

Mr. Larry Mandel
January 9, 2002
Page 6

Management Response

We concur. CITS will implement the user password expiration features as recommended on at least one of the current servers (Sage) by January 31, 2002 and the features will be implemented and enforced on all new UNIX Systems as they are installed.

TRUST FUNDS

Recommendation 13

We recommend that the Office of the Chancellor strengthen procedures over trust fund administration to ensure that all trust projects have complete agreements on file.

Management Response

We concur. Annually, the Office of the Chancellor will review all trust accounts to ensure a completed agreement is on file for all active trust accounts.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

January 24, 2002

CHANNEL ISLANDS

CHICO

MEMORANDUM

DOMINGUEZ HILLS

FRESNO

TO: Larry Mandel
University Auditor

FULLERTON

FROM: Charles B. Reed
Chancellor

HAYWARD

HUMBOLDT

SUBJECT: Draft Final Report Number 01-07 on *FISMA*,
Office of the Chancellor

LONG BEACH

LOS ANGELES

In response to your memorandum of January 24, 2002, I accept the response as submitted with the draft final report on *FISMA*, Office of the Chancellor.

MARITIME ACADEMY

MONTEREY BAY

CBR:amd

NORTHRIDGE

Enclosure

POMONA

SACRAMENTO

cc: Richard P. West, Executive Vice Chancellor and Chief Financial Officer

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSE

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS