

FISMA

HUMBOLDT STATE UNIVERSITY

Report Number 02-44

April 25, 2003

Members, Committee on Audit

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

Staff

University Auditor: Larry Mandel
Senior Director: Janice Mirza
IS Audit Manager: Gregory Dove
Senior Auditors: John Kim and Mike 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

Fiscal Information Technology..... 5

 Disaster Recovery Plan..... 5

 Data Center Intrusion Detection..... 6

 UNIX Password Controls..... 6

 VMS User Account Removal..... 7

APPENDICES

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

ABBREVIATIONS

HSU	Humboldt State University
CSU	California State University
DRP	Disaster Recovery Plan
FISMA	Financial Integrity and State Manager's Accountability Act
IT	Information Technology
SAM	State Administrative Manual
SUAM	State University Administrative Manual

INTRODUCTION

PURPOSE

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

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

SCOPE AND METHODOLOGY

The management review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor policies, letters, and directives. For those audit tests that required annualized data, fiscal year 2001-2002 was the primary period reviewed. In certain instances, we were concerned with representations of the most current data—in such cases, the test period was July 2002 to February 2003. Our primary focus was on internal controls. Specifically, we reviewed and tested:

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

INTRODUCTION

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

We have not performed any auditing procedures beyond the date of our report. Accordingly, our comments are based on our knowledge as of that date. Since the purpose of our comments is to suggest areas for improvement, comments on favorable matters are not addressed.

BACKGROUND

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

This report represents our biennial review.

OPINION

We visited the Humboldt State University (HSU) campus from January 6, 2003, through February 14, 2003, and made a study and evaluation of the accounting and administrative control in effect as of February 14, 2003. Our study and evaluation were conducted in accordance with the Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors, and included the audit tests we considered necessary in determining that accounting and administrative controls are in place and operative.

HSU 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 did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on the accounting and administrative controls. However, we did identify other reportable weaknesses that are described in the executive summary and body of this report.

In our opinion, the accounting and administrative control at HSU in effect as of February 14, 2003, 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.

FISCAL INFORMATION TECHNOLOGY [5]

DISASTER RECOVERY PLAN [5]

The university computing services department had developed an information technology (IT) disaster recovery plan (DRP) to ensure that data would be available for recovery; however, end-user recovery procedures had not been developed. With a detailed IT DRP and corresponding business continuation procedures, the campus will 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.

DATA CENTER INTRUSION DETECTION [6]

The campus did not have intrusion detection equipment to monitor unauthorized access to the data center after business hours. After hour intrusion detection equipment reduces the risk of unauthorized access during non-business hours and protects equipment and data essential to the continued operation of the campus.

UNIX PASSWORD CONTROLS [6]

Passwords controls for accounts on the production UNIX system were not set to effectively deter unauthorized access. Proper password control and enforcement improve password confidentiality and logon accountability.

VMS USER ACCOUNT REMOVAL [7]

User accounts existed on the financial computer system that did not expire and some had not been accessed in over two years. Adequate controls over account expiration and removal reduce the risk of unauthorized users gaining access to campus systems and confidential data.

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

FISCAL INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

The university computing services department had developed an information technology (IT) disaster recovery plan (DRP) to ensure that data would be available for recovery; however, end-user recovery procedures had not been developed.

State Administrative Manual (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 information technology services stated that IT disaster recovery plans were in place, but they did not include business unit manual operating procedures or subsequent data recovery and resumption procedures.

Without both a detailed IT DRP that addresses all critical systems and corresponding business continuation procedures, 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 1

We recommend that the campus 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 lost data and procedures for entering data collected manually during a prolonged system outage.

Campus Response

We concur. The campus will develop an operating and recovery procedures manual to assist business units collect and recover data during an extended outage of data processing services.

This manual will be completed by August 29, 2003.

DATA CENTER INTRUSION DETECTION

The campus did not have intrusion detection equipment to monitor unauthorized access to the data center after business hours.

We noted that although the computer room had a large number of windows, intrusion detection equipment had not been installed to detect unauthorized access after business hours.

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

The interim manager of university computing services stated that all access to the computer room had recently been reviewed, locks had been changed in August 2002, and access codes were updated in November 2002; however, no provisions had been made for monitoring after hour access.

Lack of after hour intrusion detection equipment increases the risk of unauthorized access during non-business hours and could cause the campus to lose equipment and data essential to the continued operation of the campus.

Recommendation 2

We recommend that the campus obtain intrusion detection equipment to monitor access to the data center during non-business hours.

Campus Response

We concur. Plant Operations has scheduled the installation of an intrusion detection system in the computer room for June 2003.

Installation will be completed by June 30, 2003.

UNIX PASSWORD CONTROLS

Passwords controls for accounts on the production UNIX system were not set to effectively deter unauthorized access.

Specifically, password syntax, history, expiration, and aging rules were not active, and the limit on unsuccessful access attempts was higher than industry norms.

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 interim manager of university computing services stated that the existing parameter settings had been in place for several years to accommodate the varying needs of the administrative users but that the requirements for those settings no longer existed due to architectural changes in the systems.

Ineffective password settings increase the likelihood that password confidentiality could become compromised and could result in unauthorized access.

Recommendation 3

We recommend that UNIX password settings be changed to minimize the risk of disclosure and unauthorized system access.

Campus Response

We concur. Password controls will be enabled on the production UNIX system. Initial values will be: history, five (5) iterations; aging/expiration, ninety (90) days; and limit on unsuccessful access attempts, three (3).

Implementation will be completed by August 29, 2003.

VMS USER ACCOUNT REMOVAL

User accounts existed on the financial computer system that did not expire and some had not been accessed in over two years.

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

The systems analyst for fiscal affairs stated that campus practices did not require removal of inactive accounts.

Inadequate controls over account expiration and removal increase the risk of unauthorized and undetected access to campus systems and confidential data.

Recommendation 4

We recommend that the campus implement automatic account expiration for unused user accounts and establish procedures to remove accounts from the system that have not been accessed within the past six months.

Campus Response

We concur. The campus has developed and installed a recurrent script to periodically monitor the VMS security file. Unused or inactive users are reported at five (5) months and removed at six (6) months.

Implementation complete.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Rollin Richmond	President
Ed Albert	Systems Analyst, Fiscal Affairs
Laurie Altizer	Administrative Support Assistant, University Police
Patricia Ambrosini	Payroll Officer, Fiscal Affairs
Joyce Baltierra	Office Manager, Contracts, Procurement and Risk Management
Leo "Bugs" Brouillard	Unix Systems Administrator, University Computing Services
Deborah Bushnell	Administrative Support Assistant, Fiscal Affairs
Jean Butler	Registrar, Office of Extended Education
Bill Cannon	Director of Information Technology Services
Carl Coffey	Vice President for Development and Administrative Services
Nick DeRuyter	Interim Manager, University Computing Services
Richard Giacolini	Director of Contracts, Procurement and Risk Management
Katherine Granfield	Systems Analyst, Fiscal Affairs
Doris Gunther	Supervisor, Accounting/Accounts Payable
Carl Hansen	Director, Office of Extended Education
Nancy Hansen	Accounting Technician
Connie Higgins	Supervisor, Cashiering and Registration
Cindi Hunt	Systems Coordinator, Human Resources
Claudette Lemon	Accountant
Rita Limmer	Cashier, Housing
Mary Ann McCulloch	Manager, Financial Aid Accounting
Paul Meyer	Property Clerk
Lynda Moore	Director, Human Resources
Wayne Perryman	Chair, Access Services Department
Lori Rudebock	Accounting Officer, Fiscal Affairs
Debra Ryerson-Replogle	Administrative Support Assistant, Fiscal Affairs
Pam Smith	Accounting Technician
Donna Sorensen	Director, Fiscal Affairs
Betsy Thomas	Accounting Technician
John Westmoreland	Supervisor, Distribution 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.



Vice President
Development & Administrative Services

May 13, 2003

RECEIVED
UNIVERSITY AUDITOR

MAY 15 2003

THE CALIFORNIA STATE
UNIVERSITY

Larry Mandel
University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802-4210

Re: FISMA Audit Report Number 02-44

Dear Mr. Mandel

Please find enclosed Humboldt State University's response to Audit Report Number 02-44, FISMA, Humboldt State University. We appreciate the effort you and your staff have made to indicate areas where our procedures could be strengthened. The campus is committed to addressing and resolving the issues noted in the audit report.

Questions regarding the responses may be directed to Donna Sorensen, Director, Fiscal Affairs at 707-826-3521 or dks2@humboldt.edu.

Sincerely,

Carl Coffey
Vice President for Administrative Affairs

Enclosure

c: Rollin C. Richmond, President, w/o enclosure
Bill Cannon, Director, Information Technology Services, w/enclosure
Donna K. Sorensen, Director, Fiscal Affairs, w/enclosure

FISMA

HUMBOLDT STATE UNIVERSITY

REPORT NO. 02-44

FISCAL INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

Recommendation 1

We recommend that the campus 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 lost data and procedures for entering data collected manually during a prolonged system outage.

Campus Response

We concur. The campus will develop an operating and recovery procedures manual to assist business units collect and recover data during an extended outage of data processing services.

This manual will be completed by August 29, 2003.

DATA CENTER INTRUSION DETECTION

Recommendation 2

We recommend that the campus obtain intrusion detection equipment to monitor access to the data center during non-business hours.

Campus Response

We concur. Plant Operations has scheduled the installation of an intrusion detection system in the computer room for June 2003.

Installation will be completed by June 30, 2003.

UNIX PASSWORD CONTROLS

Recommendation 3

We recommend that UNIX password settings be changed to minimize the risk of disclosure and unauthorized system access.

Campus Response

We concur. Password controls will be enabled on the production UNIX system. Initial values will be: history, five (5) iterations; aging/expiration, ninety (90) days; and limit on unsuccessful access attempts, three (3).

Implementation will be completed by August 29, 2003.

VMS USER ACCOUNT REMOVAL

Recommendation 4

We recommend that the campus implement automatic account expiration for unused user accounts and establish procedures to remove accounts from the system that have not been accessed within the past six months.

Campus Response

We concur. The campus has developed and installed a recurrent script to periodically monitor the VMS security file. Unused or inactive users are reported at five (5) months and removed at six (6) months.

Implementation complete.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSF

May 23, 2003

CHANNEL ISLANDS

CHICO

MEMORANDUM

DOMINGUEZ HI

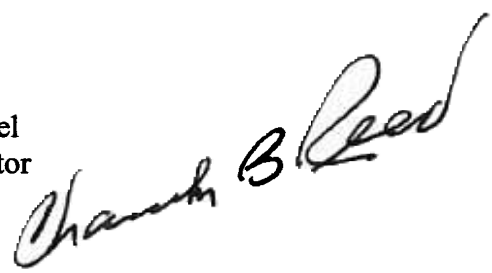
FRESNO

TO: Mr. Larry Mandel
University Auditor

FULLERTON

HAYWARD

FROM: Charles B. Reed
Chancellor



HUMBOLDT

LONG BEACH

SUBJECT: Draft Final Report Number 02-44 on *FISMA*,
Humboldt State University

MARIANA

MARITIME ACADEMY

In response to your memorandum of May 23, 2003, I accept the response as submitted with the draft final report on *FISMA*, Humboldt State University.

MONTEREY

NORTH RIDGE

POMONA

CBR/ac

SACRAMENT

Enclosure

SAN BERNARDINO

cc: Dr. Rollin Richmond, President

SAN DIEGO

SAN FRANCISCO

SAN JOSE

SAN JUAN BAPTIST

SAN MARCOS

SONOMA

STANISLAUS