OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Minnesota State Colleges and Universities

SCUPPS Information Technology Audit

JUNE 19, 2003 **03-33**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota State government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately fifty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year and one best practices review.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of Representatives and Senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 651-296-1727 (voice), or the Minnesota Relay Service at 651-297-5353 or 1-800-627-3529.

All OLA reports are available at our Web Site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, evaluation, or best practices review, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

Representative Tim Wilkin, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Dr. James H. McCormick, Chancellor
Minnesota State Colleges and Universities

Members of the Minnesota State Colleges and Universities Board of Trustees

We have conducted an information technology audit of selected areas of the State Colleges and Universities Personnel and Payroll System. Our audit scope assessed the adequacy of selected general and application controls. The individual chapters of this report discuss our specific audit objectives and conclusions.

We conducted our audit in accordance with *Government Auditing Standards*, as issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of management controls relevant to the audit. The standards require that we design the audit to provide reasonable assurance that Minnesota State Colleges and Universities (MnSCU) complied with provisions of laws, regulations, contracts, and grants that are significant to the audit. The management of MnSCU is responsible for establishing and maintaining the internal control structure and complying with applicable laws, regulations, contracts, and grants.

This report is intended for the information of the Legislative Audit Commission, the management of MnSCU, and the members of the MnSCU Board of Trustees. This restriction is not intended to limit the distribution of this report, which was released as a public document on June 19, 2003.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia Gudvangen

Claudia Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: March 31, 2003

Report Signed On: June 17, 2003

Room 140, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Brad White, CPA, CISA	Audit Manager
Eric Wion, CPA, CISA	Auditor-In-Charge
Mark Mathison, CPA, CISA	Auditor
Susan Kachelmeyer, CPA, CISA	Auditor

Exit Conference

We discussed the findings and recommendations with the following representatives of the Office of the Chancellor at the exit conference held on May 28, 2003:

Ken Niemi	Vice Chancellor – Information Technology and Chief Information Officer
Joanne Chabot	Deputy Chief Information Officer
Bev Schuft	Information Systems Manager
Laura King	Vice Chancellor – Chief Financial Officer
Bill Tschida	Vice Chancellor – Human Resources
John Asmussen	Executive Director of Internal Auditing
Beth Buse	Deputy Director of Internal Auditing
Margaret Jenniges	Director of Financial Reporting
Denise Kirkeby	Financial Reporting Supervisor

Minnesota State Colleges and Universities
SCUPPS Information Technology Audit

Report Summary

General Security Control Conclusions

In general, SCUPPS application security controlling access by campus users was found to be adequate. However, internal security weaknesses in the operating system and database management system expose MnSCU's business data, including campus payroll and personnel data, to significant risks. Many of these weaknesses were reported in 1997 and again in 2000. Specifically:

- MnSCU has not established standards for granting access to its IT professionals. IT staff were found to have excessive system privileges and too many had ability to update security transactions.

- In addition, certain SCUPPS computer programs are not properly and consistently secured, certain users could alter or delete data in uncontrolled ways, effective password management practices and monitoring methods were weak, and data transferred between SCUPPS and SEMA4 was not encrypted.

Application Control Conclusions

Generally, SCUPPS accurately processed data once it was input into the system. However, we feel MnSCU can improve controls if it designs and implements more preventative edits or automated controls. We found the system lacked several key edits. Of most significance, the system does not limit faculty and administrators pay to the negotiated bargaining agreement amounts. As a result of few preventative controls, MnSCU placed significant reliance on manual detective controls at each of its institutions. MnSCU could do more, however, to focus campus attention to unedited and high-risk transactions. Other concerns noted the need for improved monitoring of transactions entered directly into SEMA4 and increased automation and accuracy of leave data maintained in SCUPPS.

Financial-Related Audit Reports address internal control weaknesses and noncompliance issues found during our audits of state departments and agencies. The scope of our work at the Minnesota State Colleges and Universities was limited to a review of MnSCU's operating systems and SCUPPS application controls that protect the integrity of its critical business and personnel data.

This page intentionally left blank.

Chapter 1. Introduction

This information technology audit assessed the adequacy of key "general" and "application" controls for the Minnesota State Colleges and Universities' (MnSCU) State Colleges and Universities Personnel and Payroll System (SCUPPS). Application controls filter out invalid data before it can be processed and ensure that remaining transactions are completely and accurately processed. Application controls include both manual procedures, such as reconciliations, as well as computerized edit programs. General controls, on the other hand, are not unique to specific computerized business systems. Instead, they apply to all business systems that operate in a particular computing environment. Computer security policies, procedures, and standards are examples of general controls. Together the general and application controls protect the integrity of MnSCU's critical business and personnel data.

SCUPPS is an integrated human resource system that is used by MnSCU's Office of the Chancellor and its 35 institutions. MnSCU developed SCUPPS to meet the unique compensation and personnel needs of its faculty and administrators. The system office's information technology professionals manage the system. During fiscal year 2002, the system was used to manage over 70,000 work assignments for over 20,000 employees. MnSCU's annual payroll expense for this period was $781 million.

Each institution stores its business data in its own database. MnSCU houses each institutional database at one of four regional data centers. Table 1-1 shows the number of databases housed at each regional data center. It also depicts the number of employees with access to SCUPPS and number of employee records managed at each data center.

Table 1-1
Total Number of Databases, SCUPPS Users, and Employee Records Served by Each MnSCU Data Center
As of March 2003

Regional Data Center	Total Number of Databases	Number of People with SCUPPS Access	Number of Employee Records Managed
Northern (Moorhead)	11	111	4,185
Central (St. Cloud)	7	106	4,140
Southern (Mankato)	8	128	5,802
Metro (St. Paul)	13	155	7,702
Total	39	500	21,829

Source: Data provided by MnSCU's information technology professionals.

The State of Minnesota uses its own personnel and payroll system, called the State Employee Management System (SEMA4). SCUPPS transmits data to and receives data from SEMA4 on a regular basis. Though SEMA4 ultimately processes the faculty and administrator payroll, it

relies completely on application controls that are applied within SCUPPS. The total faculty and administrator payroll expense was approximately $579 million for fiscal year 2002.

Payroll, personnel, and leave records for classified MnSCU employees, who are not faculty or administrators, are subject to controls in both the SCUPPS and SEMA4 applications. SEMA4 application controls for MnSCU's classified employees are the same as applied to the rest of the state's workforce. In 2002, we performed an information technology audit of SEMA4. That report, Legislative Audit Report 02-57, concluded SEMA4-related controls were adequate. Payroll expense for MnSCU classified employees was approximately $202 million for fiscal year 2002.

Chapters 2 and 3 discuss the scope, objectives, and methodology that we used to assess the adequacy of key general and application controls. We obtained our evaluation criteria from the Control Objectives for Information and Related Technology (COBIT), published by the Information Systems Audit and Control Foundation. The COBIT Framework includes 34 high-level control objectives and 318 detailed control objectives, grouped in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring.

Chapter 2. SCUPPS Security Controls

Chapter Conclusions

SCUPPS application security controlling campus users access was found to be adequate; however, ineffective internal security controls over MnSCU's information technology professionals exposes campus data, including payroll and personnel data, to significant risks. We reported many of these weaknesses in information technology reports issued in 1997 and again in 2000. Specifically, MnSCU has not established standards for granting access to its IT professionals. IT staff were found to have excessive system privileges and too many had ability to update security transactions. In addition, certain SCUPPS computer programs are not properly and consistently secured, certain users can alter or delete data in uncontrolled ways, password management practices and monitoring methods were weak, and interface of data between SCUPPS and SEMA4 was not encrypted.

Three security software packages work together to protect critical SCUPPS data:

- **Operating System.** This software authenticates the identity of people who try to access the computers at each regional data center. The operating system also prevents unauthorized people from accessing the database and critical programs that underlie MnSCU's business systems, including SCUPPS. The MnSCU Office of the Chancellor is responsible for implementing and maintaining operating system security.

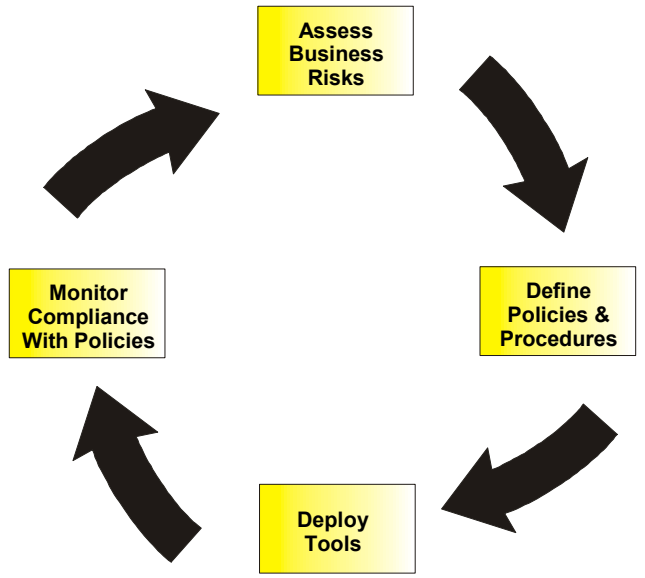
- **Database Management System.** When properly configured, the database management system prevents people from directly connecting to the database without using the appropriate SCUPPS screens. The Office of the Chancellor is responsible for implementing and maintaining database management system security.

- **SCUPPS Application Security.** Customizable security groups within SCUPPS limit people to the specific computer screens that they need to use to fulfill their job duties. The Office of the Chancellor is responsible for implementing and maintaining SCUPPS security groups. However, each institution is responsible for determining the security needs of its employees who use the system.

Powerful operating system privileges give users the ability to circumvent or bypass any security controls at all three levels described above. Similarly, powerful database management system privileges give users the ability to bypass database management system security controls.

Every organization needs strong security controls to protect its critical business data. However, even with strong controls, it is impossible to be completely secure. This fact makes designing and implementing a security infrastructure an ongoing exercise in risk management, much like buying insurance. As illustrated in Figure 2-1, organizations typically begin this process by performing a detailed risk analysis to identify potential vulnerabilities. The results of this analysis help organizations design policies and procedures to reduce their exposures to a level that executive management is willing to accept. Security professionals then deploy tools, such as access control software, to enforce the policies and procedures that were sanctioned by management. Information provided by these tools helps organizations monitor compliance with their policies and procedures and fine-tune subsequent risk assessments in the ongoing security management lifecycle. These are fundamental activities that allow an organization to effectively manage its information security risks, rather than react to individual problems in an ad hoc manner only after a violation has been detected or an audit finding has been reported.

Figure 2-1
The Ongoing Security Management Lifecycle



Source: Auditor prepared.

MnSCU's computing environment is very complex. The various layers of security and use of multiple data centers makes it challenging for MnSCU to manage its application software and users accessing its data.

In 2000, we conducted an audit that focused primarily on operating system and database management system security. That audit concluded, *"Every campus' critical business data is at risk because MnSCU does not have an effective security infrastructure to ensure that access to system resources and data is sufficiently restricted."* Previous to that, in 1997, we also came to a similar conclusion.

MnSCU has taken steps to improve security, including creating the Office of Security in 2000. The Office of Security is responsible for developing and implementing MnSCU's information security program. At the time of our audit in 2000, the Office of Security consisted of a part-time Director and one full-time staff person. In October 2001, a full time Director was hired. Since then, the office has made improvements in several areas, including application security and implementation of firewalls systemwide. It has also developed a series of draft documents, including a security policy and several broad security procedures and standards.

Audit Objective and Methodology

Our general control work focused on the adequacy of SCUPPS security controls. Specifically, we designed our work to answer the following question:

- Did MnSCU design and implement general security controls to protect the integrity of critical SCUPPS payroll and personnel data?

To answer this question, we interviewed MnSCU information technology professionals. We also reviewed security documentation developed by the agency and provided by security software vendors. Finally, we used a variety of different computer-assisted auditing tools to analyze MnSCU security data.

Conclusions

SCUPPS application security controlling campus users was found to be adequate, however, ineffective security controls over information technology professionals exposes campus data, including payroll and personnel data, to significant risks. We reported many of these weaknesses in information technology audit reports issued in 1997 and again in 2000. Specifically, MnSCU has not established standards for granting access to its IT professionals. IT staff were found to have excessive system privileges and too many had ability to update security transactions. In addition, certain SCUPPS computer programs are not properly and consistently secured, certain users can alter or delete data in uncontrolled ways, password management practices and monitoring methods were weak, and interface of data between SCUPPS and SEMA4 was not encrypted.

Table 2-1 describes key security control identified during our audit, tests that we performed to assess the adequacy of those controls, and our testing results.

Table 2-1
General Control Testing Summary

Control	Test Performed	Test Result
Predefined SCUPPS security groups limit access to specific screens.	Examine selected security groups to determine if they provide access to screens that would let employees perform unnecessary or incompatible system functions.	In general, the predefined SCUPPS security groups were designed to promote separation of duties. One security group may, however, provide unnecessary or incompatible access. Also, five people were provided excessive system-wide access because a SCUPPS security group did not exist to limit them to only the system functions they needed.
People are granted access to SCUPPS screens through security groups.	Verify users only have access to SCUPPS screens via security groups.	In general, the majority of users were granted access to screens via security groups. A few did, however, have direct access to some screens.
Predefined SCUPPS security groups provide the same level of access across each institution's database.	Compare, across each database, the access provided by each security group.	In general, the predefined SCUPPS security groups provided consistent access across all databases. We did, however, identify many obsolete groups across most databases.
System-wide SCUPPS access is limited to certain employees who need such clearance.	Identify employees with system-wide access and determine if those people need such clearance.	In general, system-wide SCUPPS access was limited to certain employees who needed such clearance.
Supervisors must approve SCUPPS security requests.	Examine SCUPPS security changes to determine if properly authorized request forms supported those changes.	SCUPPS security changes were properly documented and authorized. However, as discussed in Finding 2, an excessive number of people were authorized to enter these security transactions.
Powerful operating system or database privileges are limited to selected employees or software that need such clearance.	Identify who has powerful privileges and determine whether those people need such clearance.	As discussed in Finding 2, powerful operating system and database privileges were granted to many people who do not need such clearance. In addition, as discussed in Finding 1, MnSCU did not have adequate procedures for granting information technology professionals access.
The ability to bypass SCUPPS, and interact directly with databases and database tables from uncontrolled environments, is limited to selected employees who need such clearance.	Identify who can directly connect to databases to update data tables and determine whether those people need such clearance.	As discussed in Finding 4, several people have been granted this access that do not need it.

Control (cont'd)	Test Performed (cont'd)	Test Result (cont'd)
Operating system security features enforce strong password-related controls.	Determine whether effective password-related controls have been implemented.	As discussed in Finding 5, MnSCU did not implement strong password-related controls.
Operating System security features limit access to critical SCUPPS data and computer programs.	Examine operating system security to identify people who can access SCUPPS computer programs and data. Determine if those employees need such clearance to fulfill their job duties.	Several people had unnecessary access to SCUPPS-related computer programs as mentioned in Finding 3. Furthermore, MnSCU did not consistently secure programs.
Operating system security features enable management to identify security-related events that warrant special attention.	Determine whether MnSCU has assessed its monitoring needs and implemented strong monitoring controls.	MnSCU has not assessed its database monitoring needs or implemented any monitoring controls. See Finding 5.
Database and operating system security features help identify security-related events that should be monitored.	Determine whether MnSCU has assessed its monitoring needs and implemented strong monitoring controls.	MnSCU has not assessed its database or operating system monitoring needs. Furthermore, it has not implemented adequate monitoring controls. See Finding 5.
Encryption technology ensures and protects data during transmission.	Determine whether MnSCU encrypts confidential data during transmission.	As discussed in Finding 6, MnSCU did not encrypt some data transferred over the internet to and from SCUPPS.

Findings and Recommendations

1. PRIOR FINDING NOT RESOLVED. MnSCU has not implemented formal standards and procedures for granting access to its information technology professionals and software.

MnSCU has not implemented standards and procedures for providing access to its information technology professionals and software. In most cases, these are the system's most powerful users.

MnSCU has not explicitly authorized or restricted anyone from entering security transactions for its information technology professionals. This is very important because many people have the ability to perform them. MnSCU has not adopted formal standards and procedures that require documentation, including proper management authorizations and statements of need, to create or

modify access. Finally, MnSCU has not implemented standards and procedures to adequately challenge and reauthorize access on a periodic basis.

These shortcomings have resulted in people and software having excessive and often very dangerous access. In Findings 2 and 3 we describe information technology professionals who have excessive system privileges and unnecessary access to important computer programs. In Finding 4, we describe people who can circumvent computer application screens and view, alter, or delete critical data from uncontrolled environments.

Recommendation

- *MnSCU should implement strong controls to ensure information technology professionals' access is authorized, limited to the minimum level necessary, documented, and periodically reviewed.*

2. PRIOR FINDING NOT RESOLVED. Many information technology professionals have unnecessary system privileges, and an excessive number are authorized to enter security transactions.

Many information technology professionals were granted various combinations of extremely powerful operating system privileges that were not needed. Examples of employees with this type of access included 14 operations staff, 6 development staff, 4 college employees, and others. In addition, many other accounts used to run computer programs had excessive privileges. Granting powerful operating system privileges to people or other accounts is extremely risky because they can bypass or circumvent security-related controls at all levels, including the operating system, database management system, and MnSCU's business systems, including SCUPPS. As a result, they can access, alter, or delete nearly any resource on the system.

At least six information technology professionals, including three development staff, were granted excessive and extremely powerful database management system privileges. These privileges are particularly risky because it gives the individuals the ability to perform database management functions and bypass or circumvent database security. As a result, they can delete entire databases or modify any data stored in them. These issues are compounded because, as described in Finding 5, MnSCU has not assessed its needs to monitor operating system and database events.

In addition, an excessive number of employees are authorized to enter security transactions for college users, including SCUPPS users. Each of the four data centers has designated one primary person for this task, as well as several people as back-ups. We feel there should be fewer individuals authorized to enter security transactions.

Recommendations

- *MnSCU should grant employees and other accounts the minimum security clearances necessary for them to perform their normal job duties.*

- *MnSCU should limit the number of individuals authorized to enter security transactions for its campus users.*

3. Some computer programs, including SCUPPS programs, are not properly or consistently secured.

Some computer programs are not properly or consistently secured. For example, programs used to enter security transactions were not properly nor consistently secured across the four data centers. As a result, many people could execute the programs, and two could actually alter or modify them. In addition, information technology staff must have a powerful privilege to activate this program, resulting in the need for excessive operating system privileges, as discussed in Finding 2.

SCUPPS-related programs were also not properly or consistently secured. For example, at least six people and three software-related accounts were given the ability to read, write, execute, and delete the programs. In addition, some of these users had the ability to modify the security permissions set on selected programs. In many cases, these users did not need any access, while in others, they needed more restrictive access. Finally, SCUPPS-related programs were not consistently secured across the four data centers.

Recommendations

- *MnSCU should properly and consistently secure its security-related programs and configure security so authorized users do not require a powerful privilege to successfully execute the programs.*

- *MnSCU should properly and consistently secure its SCUPPS programs.*

4. PRIOR FINDING NOT RESOLVED. Several users can view, alter, or delete critical data from uncontrolled environments.

Generally, computer system users view, alter, or delete data by using each application's screens designed by MnSCU. These computer screens are designed with numerous program logic edits. The edits are extremely important because they protect the integrity of data that flows into each institution's database. Unfortunately, several users can circumvent these edits by viewing, updating, or deleting data without using the appropriate ISRS screens. We found at least 30

people with such access, although their jobs did not require it. Eleven users could only view information; however, 19 could alter or delete data.

Risks are further compounded since several individuals have very powerful privileges allowing security to be bypassed and because of the lack of monitoring procedures for operating system and database security-related events. In addition, MnSCU did not implement formal change control procedures in its database environments. Change controls are extremely important because they ensure that only authorized people make changes to data.

Recommendations

- *MnSCU should limit who can interact with databases and database tables from uncontrolled environments.*

- *MnSCU should implement stronger change controls in its database environment.*

5. MnSCU did not enforce strong password management controls.

MnSCU did not implement effective password management practices. These controls are important because they force people to select hard-to-guess passwords that have not been used previously and must be changed periodically. In addition, controls can disable accounts that are a target of a break-in attempt. In some cases, MnSCU did not implement controls, and in others they were implemented, but some individual accounts were allowed to circumvent them. We were also told that people shared some of the most powerful accounts. Strong password controls are critical because a password is generally the only thing to prevent someone from gaining unauthorized access.

Recommendation

- *MnSCU should implement and enforce strong password management controls.*

6. PRIOR FINDING NOT RESOLVED. MnSCU does not have effective monitoring of security-related events.

MnSCU did not implement strong monitoring controls. It has not assessed its needs to monitor both operating system and database security-related events. Currently some operating system events are logged, however, the logs were not consistently reviewed or not reviewed at all. Currently, no database events are logged and monitored. Monitoring controls are important because they are designed to detect security-related events that may be unauthorized.

Recommendation

- *MnSCU should assess its monitoring needs and implement stronger monitoring controls over security-related events.*

7. Some interface files were not appropriately secured during transmission.

Some data transferred to and from SCUPPS was not encrypted. Data transfers between SEMA4 and SCUPPS take place over public networks. Unfortunately, many tools allow unscrupulous people to capture transmissions that occur over public networks. Though encryption does not prevent eavesdropping, it makes it extremely difficult for hackers to decipher any hijacked transmissions. This same issue was reported to the Departments of Employee Relations and Finance in our Legislative Audit Report 02-57, *SEMA4 Information Technology Audit*, issued in August 2002. Implementation of encryption software will require coordination between MnSCU and the departments that manage SEMA4.

Recommendation

- *MnSCU should work with the Departments of Employee Relations and Finance to encrypt transmissions between SCUPPS and SEMA4.*

This page intentionally left blank.

Chapter 3. SCUPPS Application Controls

Chapter Conclusions

Generally, SCUPPS accurately processed data once it was input into the system. However, we feel MnSCU can improve controls if it designs and implements more preventative edits or automated controls. We found the system lacked several key edits. Of most significance, the system does not limit faculty and administrator pay to the negotiated bargaining agreement amounts. In fact, the system will accept and pay any dollar amount. As a result of having few preventative controls, MnSCU placed significant reliance on manual detective controls at each of its institutions. Typically, this includes scrutiny and review of system reports. MnSCU could do more, however, to alert campus users to unedited or high-risk transactions. Other concerns included the need for improved monitoring of transactions entered directly into SEMA4 without being first updated in SCUPPS and improved automation of severance liquidations and personal day accruals.

SCUPPS is used by MnSCU to process personnel transactions and calculate pay rates for its employees. SCUPPS data is periodically transferred to the state's payroll and personnel system, SEMA4, to process paychecks. SEMA4 payroll expenditures are summarized and posted to the state's accounting system called MAPS. SEMA4 data is also transferred back to SCUPPS, and payroll expenditures are posted into MnSCU's accounting system.

Application controls filter out invalid data before it can be processed and ensure that remaining transactions are completely and accurately processed. Application controls include both manual procedures, such as reconciliations, as well as computerized edit programs. When practical, computerized controls are preferred over manual controls because computerized controls can be applied more consistently and accurately. Application controls can be preventative or detective in nature. Preventative controls are often desired because they stop invalid data or transactions from occurring. Detective controls, on the other hand, are applied after-the-fact.

Implementing SCUPPS application controls is not a trivial task. In fact, it can be very complex. The complexity of faculty and administrator's bargaining agreements is one factor that makes it more challenging. For example, faculties at four-year universities have different bargaining agreements than faculties employed at two-year colleges. Furthermore, the compensation criteria is different for each bargaining agreement. In some cases, the compensation criteria is even different among faculty in the same bargaining agreement. Faculty may be employed at multiple institutions, further complicating the matter.

Audit Objective and Methodology

Our application control work focused on the adequacy of pay rate and payroll processing controls. Because payroll and personnel transactions for MnSCU's classified staff were subjected to edits and controls we previously tested in SEMA4, our audit work focused mainly on MnSCU's unclassified faculty and administrators. Specifically, we designed our work to answer the following question:

- Did MnSCU design and implement adequate input, processing, and output controls?

To answer this question, we interviewed information technology, human resource, and payroll professionals at the Office of the Chancellor and at select colleges. We also reviewed relevant documentation and used computer-assisted audit tools to analyze and test significant controls.

Conclusions

Generally, SCUPPS accurately processed data once it was input into the system. However, we feel MnSCU can improve controls if it designs and implements more preventative edits or automated controls. We found the system lacked several key edits. Of most significance, the system does not limit faculty and administrator pay to the negotiated bargaining agreement amounts. In fact, the system will accept and pay any dollar amount. As a result of having few preventative controls, MnSCU placed a significant reliance on manual detective controls at each of its institutions. Typically, this includes scrutiny and review of system reports. MnSCU could do more, however, to alert campuses users to unedited or high-risk transactions. Other concerns included the need for improved monitoring of transactions entered directly into SEMA4 without being first updated in SCUPPS and improved automation of severance liquidations and personal day accruals.

Table 3-1 describes key security controls identified during our audit, tests that we performed to assess the adequacy of those controls, and our testing results.

Table 3-1
Application Control Testing Summary

Control	Test Performed	Test Result
Internal SCUPPS tables ensure that faculty and administrators' work assignments total the dollar amounts stipulated by applicable bargaining agreement's compensation grids.	Verify the base salaries and pay rates in SCUPPS' internal control tables agree, on a sample basis, with negotiated agreements.	SCUPPS internal tables agreed with bargaining agreement grids. However, we found that internal SCUPPS tables were not used to control manual work assignments nor "off-step" assignments. Finding 8 discusses how edits and exception reports could improve assurances.
	Verify that internal control tables adequately restrict a sample of specific job classes to the appropriate bargaining agreement's compensation grids.	Employee job classifications limit allowable compensation grids.
	Verify the internal tables are consistent across each institution's database.	The internal tables were found to be consistent across each institution's database.
College staff enter the scheduled pay amount disbursed for each employee. System edits compare the amount scheduled to be disbursed to the work assignment amount.	Review the computerized edit.	Although the system displays a warning if there is a difference between the scheduled disbursement and work assignment amounts, the system will process the transaction. In fact, the system will accept any amount to be scheduled for disbursement. Finding 8 suggests that edits could improve attention to differences.
SCUPPS programs calculate an employee's compensation for an assignment.	For material assignment types, recalculate assignment amounts for all faculty.	Assignment amounts were independently recalculated with no differences noted.
SCUPPS uses assignments to prompt an encumbrance of funds in accounting.	Verify and observe that assignment dates prompt a payroll encumbrance.	Assignments prompted a MnSCU accounting encumbrance based on an academic year rather than on an accounting fiscal year from July 1 to June 30. However, manual adjustments are properly made to accrue payroll expenses into the correct fiscal year.
MnSCU requires human resource transactions to be entered in SCUPPS for interface to SEMA4. MnSCU monitors those transactions entered directly by campuses into SEMA4.	Determine the effectiveness and extent of MnSCU's monitoring of human resource transactions directly entered into SEMA4.	As discussed in Finding 9, MnSCU needs to improve its monitoring process, prohibit certain transaction types, and enforce campus compliance.

Control (cont'd)	Test Performed (cont'd)	Test Result (cont'd)
SCUPPS computer programs accurately calculate vacation, sick, and personal leave balances for faculty and administrators.	Discuss leave accrual program logic and observe leave reports to determine whether the system accurately maintains leave hours.	SCUPPS accurately maintains leave balances for full-time faculty and administrators. However, as discussed in Finding 10, concerns were noted with lack of automated reduction of leave at termination, accuracy of leave for part-time faculty, and the need to manually activate the SCUPPS leave module.

Findings and Recommendations

8. MnSCU did not design and implement some key system edits.

MnSCU did not design and implement some key computerized edits. Of most significance, the system will accept and process any pay rate for faculty or administrators. In some cases, a warning message will display to indicate a potential error; however, the transaction can be processed and the amount paid. During fiscal year 2002, faculty and administrators accounted for approximately 74 percent of MnSCU's total payroll.

Most employees have a pay rate that corresponds to an amount in a bargaining agreement's compensation grid. Compensation grids identify the pay rate ranges for a given job. Each range contains several steps or individual pay rates. MnSCU maintains the compensation grids in an internal SCUPPS table. However, MnSCU did not implement automated edits to compare the input pay rate to the applicable compensation grid to ensure the amount paid was accurate. Rather, MnSCU's emphasis was placed on manual detective controls at each of its 35 institutions, mainly providing campus management and users with numerous reports to scrutinize and review for accuracy.

Some employees can be paid a rate that is different from those included in a compensation grid. The term to describe these situations is "off step". Generally these employees are off step because their pay rates do not land directly on a step within a range. The rate, however, must be within the pay rate range for the given job. Approximately 25 percent of MnSCU employee assignments are off step. MnSCU did not implement automated edits to ensure people's pay rates did not exceed the maximum step or pay rate for the given job and pay range. Although rare, some people who are off step can be paid a rate that exceeds the maximum for the given job and pay range. Even with automated edits, off step transactions should be manually reviewed on a routine basis for authorization and appropriateness.

MnSCU uses work assignment codes to identify the type of work being performed by its employees. For example, instructional work assignments are generally used for faculty who teach courses. In addition, assignment types also play an important role in calculating people's pay. For example, overload assignment codes are used to identify faculty who teach more credit hours than what the bargaining agreement requires. MnSCU did not, however, implement

automated controls to ensure work assignment codes properly reflect the actual type of work performed by the employee. SCUPPS allows any assignment code to be assigned to any employee without any computerized edits. As a result, the assignment code used may not reflect the actual work or tasks performed. . Ideally, users should be alerted to potentially miscoded or illogical assignments.

As a result of having few preventative controls, MnSCU placed significant reliance on manual detective controls at each of its institutions. Typically, this includes scrutiny and review of system reports. The development of certain technology controls and edits may impact certain transaction risks causing the need for diminished or expanded detective review by campuses**.** MnSCU should assess transaction risks while developing edits and consider improvements in campus detective controls by focusing attention on unedited or high-risk transactions. MnSCU has developed numerous SCUPPS reports for human resource and payroll activities. Some management reports extract and sort the full population of SCUPPS data being queried, while others are exception reports. MnSCU could do more, however, to alert campuses users to unedited or high-risk transactions. For example, newly hired employees, over and under payments, and changes to pay rates are deserving of greater scrutiny.

Recommendations

- *MnSCU should assess its need to design and implement more SCUPPS edits, including those that:*
  - *compare faculty and administrator's pay rates to the amounts authorized in the various bargaining agreement compensation grids; and*
  - *ensure that work assignments are accurately and properly used.*

- *MnSCU should implement procedures to routinely review off step pay rates to ensure they are authorized and appropriate.*

- *MnSCU should prepare a SCUPPS-related risk assessment and consider ways to improve campus detective controls to effectively focus on unedited or high-risk personnel and payroll transactions.*

9. MnSCU needs to better monitor human resource transactions entered directly into SEMA4.

MnSCU routinely transmits SCUPPS data to the state's payroll and personnel system, SEMA4. MnSCU developed computerized edits to help ensure this data successfully posts into SEMA4. However, campus staff can circumvent these controls by bypassing SCUPPS and entering transactions directly into SEMA4. Although a few types of transactions must always be entered directly into SEMA4, most should not. The MnSCU Office of the Chancellor has communicated its concerns to campuses and directed them to discontinue entering unnecessary transactions directly into SEMA4. During our audit, we noted that MnSCU campuses processed approximately 1,500 to 3,000 transactions per month directly into SEMA4. It was not possible

to distinguish between transactions that were required to be directly entered and those that were not.

Although the MnSCU Office of the Chancellor performs some monitoring of these activities, we feel monitoring controls could be improved. MnSCU routinely runs reports to identify the number of transactions each person directly enters into SEMA4. Another strategy that MnSCU should employ would be to identify the specific transaction types that should not be entered directly into SEMA4 and implement procedures to identify them and assess their appropriateness.

While improved monitoring may lessen the number of these transactions, MnSCU may need to explore additional alternatives to forcing compliance. For example, policies or procedures could explicitly prohibit college staff from entering unnecessary transactions directly into SEMA4. If direct entry continues, personnel action could be prompted for noncompliance.

Recommendation

- *MnSCU should implement more stringent monitoring controls to ensure direct entries into SEMA4 are appropriate.*

10. SCUPPS does not accurately accrue or maintain leave for part-time faculty, and users must manually reduce or adjust leave balances upon separation.

MnSCU uses SCUPPS to control and manage paid leave to faculty and administrators for vacation, sick, or personal days. Vacation and sick leave paid upon termination is used to determine each college's compensated absences liability. Personal leave days are not paid at termination, but a limit exists on the maximum days an employee can carryover from one year to the next. We found some areas where SCUPPS does not automatically maintain or accurately accrue leave as discussed below.

- SCUPPS vacation and sick leave balances are not automatically reduced upon payment of vacation payoff and severance, nor has the system been designed to quantify leave liability for severance payments funded over multiple years. Colleges and universities are required to manually reduce leave balances when faculty and administrators terminate. We detected one campus that neglected to post this reduction of hours upon separation, causing an overstatement of their compensated absences liability for the past several years.

- Personal leave days for certain part-time faculty employed at two-year colleges are not automatically accrued. As a result, institutions are required to manually calculate the accruals and adjust SCUPPS accordingly. Also, SCUPPS does not accrue personal days for two-year colleges at the correct maximum level. We noted instances where the system limit was different than the specified contract maximum. In these cases, faculty were entitled to one more personal day than was recorded by the system.

- College staff are also required to manually activate SCUPPS computer programs to accrue leave and calculate leave balances. Generally, these types of computer programs are

scheduled to run automatically every pay period to ensure leave records are adjusted in a timely manner.

Recommendation

- *MnSCU should consider improvements and accuracy in SCUPPS leave processing by:*
  - *automatically reducing or adjusting leave balances upon termination;*
  - *accurately accruing and maintaining maximum personal leave days for faculty employed at two-year colleges; and*
  - *scheduling leave-related computer programs to run automatically every pay cycle.*

This page intentionally left blank.

Status of Prior Audit Issues
As of March 31, 2003

Most Recent Information Technology Audits

Legislative Audit Report 00-53, issued in November 2000, was a follow-up of a 1997 security audit of system-wide access to MnSCU data. We found that MnSCU business data continued to be at risk because the system has not formally defined its security infrastructure. Recommendations were repeated in this report.

Legislative Audit Report 97-46, issued in August 1997, involved a selected-scope security audit of MnSCU information systems. We raised concerns about access to the systems from unauthorized environments, ineffective procedures for managing user accounts, inadequate control over powerful system privileges and security groups, and ineffective security monitoring procedures. A few of these concerns were not resolved and are repeated in this report.

State of Minnesota Audit Follow-Up Process

The Department of Finance, on behalf of the Governor, maintains a quarterly process for following up on issues cited in financial audit reports issued by the Legislative Auditor. Finance has delegated this responsibility for all Minnesota State Colleges and Universities (MnSCU) audit findings to the MnSCU Office of Internal Auditing. MnSCU's Office of Internal Auditing's process consists of quarterly activity reports documenting the status of audit findings. The follow-up process continues until the Office of Internal Auditing is satisfied that the issues have been resolved.

This page intentionally left blank.

MnSCU

Minnesota State Colleges & Universities

June 16, 2003

James R. Nobles
Legislative Auditor
Office of the Legislative Auditor
Centennial Building 658 Cedar Street
St. Paul MN 55155

Dear Mr. Nobles,

This is in response to the information technology audit of the Minnesota State Colleges and Universities Personnel Payroll System (SCUPPS). We appreciate the efforts of the audit staff and their interest in working with us to improve our operations. The information they provide helps improve the data integrity, operations and security of the system for all users. We feel strongly that our current security infrastructure and policies provide a reasonable level of security for our systems and data. We do agree, however, that it is imperative that we continue to enhance and improve our security policies, infrastructure and operations. Our response to your recommendations which follows delineates our plan to carry out those enhancements. We look forward to ongoing communication with your staff on our efforts to implement your recommendations in an effective manner.

The events of 9/11 have resulted in a dramatic change in our security focus. Prior to those events, we were aggressively working toward implementation of recommendations consistent with audit findings. Following 9/11, we made a deliberate decision to place priority emphasis on efforts designed to prevent outside exploitation of our networks. This approach complied with recommendations from the Office of Homeland Security, but we believe it also added significantly to the fundamental security of our application systems.

Unfortunately, the state budget crisis and subsequent funding reductions and loss of positions have been a challenge affecting our ability to move as rapidly as we would like on all projects. Our primary responsibility is to maintain our ability to provide systems and services in support of Minnesota State Colleges & Universities' campuses and students, and we have made that responsibility our highest priority. As part of that responsibility, we have made considerable progress toward resolving outstanding audit findings, which we have detailed in our individual responses to your report findings.

Some of the activities that were undertaken to address previous findings include:

- Draft procedures for granting and reviewing access rights for ITS staff are developed and ready for implementation.

- Reports are now created and sent to HR directors at all campuses each pay period, identifying employee job status changes that may affect security privileges. Data center staff automatically remove access rights for employees leaving a campus or the system.

- ISRS security reports have been developed for each campus and ISRS module. These are now made easily available in the Data Warehouse using Brio. Flag identifiers have been added to security reports to make identification of staff classification easier.

- Workgroups are identifying incompatible rights and establishing guidance for colleges and universities to use when reviewing individual user access on ISRS, SEMA4 and MAPS, and controls to address them. The first report was received from the Accounts Receivable workgroup in May.

- Significant progress has been made toward creating a comprehensive MnSCU wide security infrastructure, based on the ISO standard ISO 17799. We believe this is a significant accomplishment, positioning MnSCU as a leader among higher education institutions throughout the country. The Model provides a consistent set of policies and standards defining minimum requirements required for implementation in each institution. Information Security Policy and Procedures, as well as standards for Data Protection, Applications, Computing Platform, Network, Systems Development and Telecommunications were drafted by the Security Steering Committee and reviewed with all campuses and data centers.

- Network firewalls were implemented system wide

- Risk Assessments were completed for ETC and the Metro Region Computing Center and started at the Central Region Computing Center. Assistance to four institutions undertaking their own assessments was also provided.

While we are eager to continue with projects to further enhance our security infrastructure, we are convinced that significant progress has been made and continues to be made. We will continue working to improve the security of our systems. Our plans to address the current audit findings are attached.

Sincerely,

/s/ Ken Niemi

Ken Niemi
Vice Chancellor for Information Technology & CIO

/s/ Bill Tschida

Bill Tschida
Vice Chancellor for Human Resources

Recommendation 1: MnSCU should implement strong controls to ensure information technology professionals' access is authorized, limited to the minimum level necessary, documented, and periodically reviewed.

Response:

- *While ITS has not had any security incidents related to this finding, draft procedures have been developed and are currently under final review which will fully document the security rights approval process for ITS staff. That process does include periodic review. In addition, role based authority and rights requirements for ITS development and operations staff have been documented and are under final review. Based on job responsibilities and access needs defined in the Role Based Security Document, unnecessary privileges will be removed and, where necessary, detective controls will be established. We plan final implementation of the complete Role Based Security System no later than December 2003.*

Recommendation 2:

- MnSCU should grant employees and other accounts the minimum security clearances necessary for them to perform their normal job duties.
- MnSCU should limit the number of individuals authorized to enter security transactions for its campus users.

Response:

As noted in the response to recommendation 1, role based responsibilities and security requirements for ITS development and operations staffs have been documented and are under final review. Security will be based on minimum levels of access needed for job responsibilities and procedures will be formalized to monitor authorization levels. The four data centers covering multiple shifts have required several staff to have rights to enter security transactions; the volume of activity is too great for a single location or individual to handle. A project to automate this function and allow for central review is being revisited and will be considered.

Recommendation 3:

- MnSCU should properly and consistently secure its security-related programs and configure security so authorized users do not require a powerful privileges to successfully execute the programs.
- MnSCU should properly and consistently secure its SCUPPS programs.

Response:

- *The OpenVMS programs (scripts) that MnSCU developed as the standard for creating and modifying VMS accounts and ISRS security tables will be moved to a secured directory in July 2003. Along with securing these programs, MnSCU will closely review the staff that have privileges to execute the security-related programs.*

- *SCUPPS application programs source code is controlled by OpenVMS source code management system. This system tracks all modifications to the source code and provides for an audit trail. The Uniface programs are controlled by MnSCU's manual change management system. Modifications to key programs are assigned to specific staff members with comprehensive knowledge of the SCUPPS system. Additionally, ITS is currently auditing the ISRS menu system to align end-user accounts with the menu groupings. This will be completed by the end of July, 2003.*

Recommendation 4:

- MnSCU should limit who can interact with databases and database tables from uncontrolled environments.
- MnSCU should implement stronger change controls in its database environment.

Response:

- *MnSCU's staffing limitations are such that work traditionally assigned to DBA staff is, of necessity, shared among several individuals. To minimize security risks inherent with this approach we have created a detective control process to track all database changes implemented. This process is in quality assurance, and will be implemented as soon as it clears final testing. The next step we will take is to improve the structure for change control within the regular weekly rollout. The role of the DBA is being documented as part of our role based security standards and procedures. While that project is not yet complete, the role for DBA access is in place. Proxy access out of development does not allow an override of security in production. We do limit the people who can do this, and will include this in a structured standard review session.*

Recommendation 5: MnSCU should implement and enforce strong password management controls.

Response:

- *The recently created MnSCU Security Standards do address password controls; however, OpenVMS does not have an edit feature to ensure that the password is in fact alphanumeric. With this exception, OpenVMS does support the standard. OpenVMS has strong security features that have been reviewed and accepted by the federal government and other security related organizations. The MnSCU security standard process does allow for exceptions which we are considering as a possibility. However, invoking the password security standard will cause some level of stress throughout MnSCU. Requiring all passwords to comply with the standard will require notification with ample time for MnSCU staff to adjust their password management practice. MnSCU will make the proper announcements and invoke the standard by August, 2003.*

Recommendation 6: MnSCU should assess its monitoring needs and implement stronger monitoring controls over security-related events.

Response:

- *The ITS Infrastructure unit will document a standard procedure to review the security logs for VMS accounts each day. The procedure used to review these account logs will be implemented by August 2003. The ITS Security Office will be notified of significant events. This process is intended as a temporary solution. The Security Office is working toward creation of a formal standard defining critical events in more detail. Once completed we will issue incident reports and adhere to the ITS Security Office's standard.*

Recommendation 7: MnSCU should work with the Departments of Employee Relations and Finance to encrypt transmissions between SCUPPS and SEMA4.

Response:

- *MnSCU is exploring several options with the Department of Administration, InterTechnologies Group, to establish an encrypting standard acceptable to both agencies. It is MnSCU's intent to have file transfer encryption fully operational by the end of July 2003.*

Recommendation 8:

- MnSCU should assess its need to design and implement more SCUPPS edits, including those that:
    - Compare faculty and administrator's pay rates to the amounts authorized in the various bargaining agreement compensation grids; and
    - Ensure that work assignments are accurately and properly used.
- MnSCU should implement procedures to routinely review off step pay rates to ensure that they are authorized and appropriate.
- MnSCU should prepare a SCUPPS-related risk assessment and consider ways to improve campus detective controls to effectively focus on unedited or high-risk personnel and payroll transactions.

Response:

- *Several months ago, a control table was created that will ultimately be used to enforce valid use of assignment types based on bargaining unit. Several additional changes to SCUPPS screens and reports are needed before implementation.*

- *MnSCU has implemented some routine procedures related to pay rate review. For example, administrators are paid based on a salary range and minimum/maximum edits have been created to ensure entering a valid salary for the range. However, there are valid reasons for allowing administrators to be paid above or below the range, so SCUPPS doesn't prevent a salary outside the range. It does issue a warning, however. Similarly, for state university faculty, job market considerations sometimes drive a deliberate decision to designate base salaries that are off step and within the published salary range. This type of flexibility is essential within the higher education environment, as acknowledged in the audit report.*

- *ITS staff will work with Human Resources to identify risk areas for SCUPPS, and establish appropriate detective controls where necessary.*

Recommendation 9: MnSCU should implement more stringent monitoring controls to ensure direct entries into SEMS4 are appropriate.

Response:

- *All requests for SEMA4 access are granted by MnSCU HR. If update access is approved, the user has the authority to enter inappropriate transactions online in SEMA4 just as they have access to enter appropriate transactions.*

- *We currently do not have access to a report showing which transactions were entered online or what data was changed. It is our understanding that MnSCU HR would have to request a report from the State that would provide them with this information. They could then use it to monitor the appropriateness of transactions entered online in SEMA4.*

Recommendation 10:

- MnSCU should consider improvements and accuracy in SCUPPS leave processing by:
  - automatically reducing or adjusting leave balances upon termination;
  - accurately accruing and maintaining maximum personnel leave days for faculty employed at two-year colleges; and
  - Scheduling leave-related computer programs to run automatically every pay cycle.

Response:

- *We are currently redesigning the leave accrual system to maintain accurate leave balances for MSCF employees. We currently have no plan to automatically run the accrual program or reduce/adjust leave balances; however, it will be further discussed with users. This would require a business process change they may prefer not to adopt.*