OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Minnesota State Colleges and Universities

Financial Reporting Information Technology Controls

JUNE 24, 2005 **05-36**

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 forty 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.

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 651-296-1235 (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, or evaluation, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

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

Senator Ann H. Rest, 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 controls relating to the preparation of the annual financial statements for the Minnesota State Colleges and Universities (MnSCU). The scope of our audit focused on application and security controls used to protect the integrity of MnSCU's computerized financial reporting system. The Report Summary highlights our overall conclusions. Our specific audit objectives and conclusions are contained in the individual chapters of this report.

We would like to thank staff from the Minnesota State Colleges and Universities for their cooperation during this audit.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: May 2, 2005

Report Signed On: June 21, 2005

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

Minnesota State Colleges and Universities
Financial Reporting Information Technology Controls

Table of Contents

Audit Participation

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

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Cecile Ferkul, CPA, CISA	Audit Manager
Mark Mathison, CPA, CISA	Auditor-in-Charge
Neal Dawson, CPA, CISA	Auditor
John Kelcher	Auditor

Exit Conference

We discussed the findings and recommendations in this report with the following staff of the Minnesota State Colleges and Universities on June 13, 2005:

Laura King	Vice Chancellor and Chief Financial Officer
Ken Niemi	Vice Chancellor – Chief Information Officer
Tim Stoddard	Assistant Vice Chancellor – Financial Reporting
John Asmussen	Executive Director – Internal Auditing
Beth Buse	Deputy Director – Internal Auditing
Margaret Jenniges	Financial Reporting Director
Bev Schuft	Information Technology Security Director
Metody Popov	Accounting Officer Principal, Financial Reporting

Report Summary

Conclusion:

The Minnesota State Colleges and Universities (MnSCU) designed and implemented many controls over its financial reporting system to ensure the accuracy and completeness of its annual financial statements. However, MnSCU could strengthen some controls to improve the efficiency of its financial reporting process and to better limit access to the financial reporting system and data.

Findings:

- MnSCU did not have a formal process to verify the initial entry of data summarized from its main accounting system. (Finding 1, page 7)
- MnSCU's financial reporting system lacked some automated edits to prevent certain data entry errors. (Finding 2, page 7)
- MnSCU did not actively monitor its list of accounts for errors or inconsistencies. (Finding 3, page 8)
- MnSCU lacked strong password controls for its financial reporting system. (Finding 4, page 10)
- Some individuals had more access to data and system resources than was necessary. (Finding 5, page 11)

The audit report contained 5 audit findings relating to internal control over MnSCU's financial reporting system.

Audit Scope:

Audit Period:
As of April 2005

Audit Scope:
MnSCU's financial reporting system:
- Selected Application Controls
- Selected Security Controls

Background:

This information technology audit assessed the adequacy of specific controls in MnSCU's computerized financial reporting system. MnSCU implemented a financial reporting system to assist with preparing consolidated and individual financial reports for its colleges and universities.

For the fiscal year ending June 30, 2004, MnSCU published a consolidated financial report for its 32 institutions. It also issued separate financial reports for 12 institutions. External audits of these financial reports resulted in unqualified audit opinions.

This page intentionally left blank.

Chapter 1. Introduction

The Office of the Legislative Auditor performs information technology audits to assess how well the controls established by state agencies protect government systems and data. This audit assessed the adequacy of specific controls designed to ensure that the Minnesota State Colleges and Universities' computerized financial reporting system accurately compiled initial financial data and accurately transferred adjusted data to the financial statements. We also assessed the adequacy of controls designed to limit access to the financial reporting system and its data. We decided to review this system and its controls because of the system's complexity and its importance in producing financial reports.

For fiscal year 2004, MnSCU prepared a systemwide financial report for its 32 institutions and separate financial statements for all seven state universities and five of its two-year colleges. These reports allowed MnSCU to provide more detailed information about its financial condition and results of operations than is included in the state's Comprehensive Annual Financial Report.[1] MnSCU's Finance Division, with assistance from the administrative and finance staff at the colleges and universities, prepared these annual financial reports in accordance with generally accepted accounting principles as prescribed by the Governmental Accounting Standards Board. External audit firms provided unqualified audit opinions which attested to the fairness of the presentation of the systemwide and individual institutions' financial reports. For the fiscal year ending June 30, 2004, MnSCU's net assets totaled $1.1 billion, and its operating revenues were $802 million.

To assist in preparing its financial reports, MnSCU purchased a financial reporting system. MnSCU used the financial reporting system to:

- consolidate transactions from its main accounting system,[2]
- adjust those transactions to comply with governmental accounting principles, and
- properly report those transactions in the financial statements.

Audit Approach

We conducted this audit in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. These standards require that we obtain an

[1] MnSCU is included in the State of Minnesota's Comprehensive Annual Financial Report as a major fund. MnSCU's financial activities represented 78 percent, 92 percent, and 35 percent, respectively, of the total assets, net assets, and operating revenues of all the state's business-type activities.

[2] MnSCU's main accounting system is the Integrated Statewide Record System (ISRS).

understanding of internal controls relevant to the audit objectives. We outline the audit objectives in Chapters 2 and 3 of this report.

For this information technology audit, we obtained evaluation criteria from a variety of sources, including:

- the Control Objectives for Information and Related Technology (COBIT);[3]
- information published by the developers of purchased computer software;
- publications distributed by recognized security experts, such as the National Institute of Standards and Technology;
- generally accepted accounting principles prescribed by the Governmental Accounting Standards Board; and
- expectations of MnSCU's management, defined in various policies, standards, and procedures.

This information technology audit included a review of security data that the Minnesota Data Practices Act legally classifies as nonpublic. To protect state resources and comply with the Minnesota Data Practices Act, we withheld specific security-related details from this publicly released report. We communicated all pertinent details to MnSCU administration in a separate, nonpublic document.

The primary audiences for this report are the Legislature, managers at the Minnesota State Colleges and Universities, and its Board of Trustees. However, we also intended for our report to assist those audit firms that attest to MnSCU's consolidated and individual institution's financial statements.

[3] Published by the IT Governance Institute, COBIT 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. Application Controls

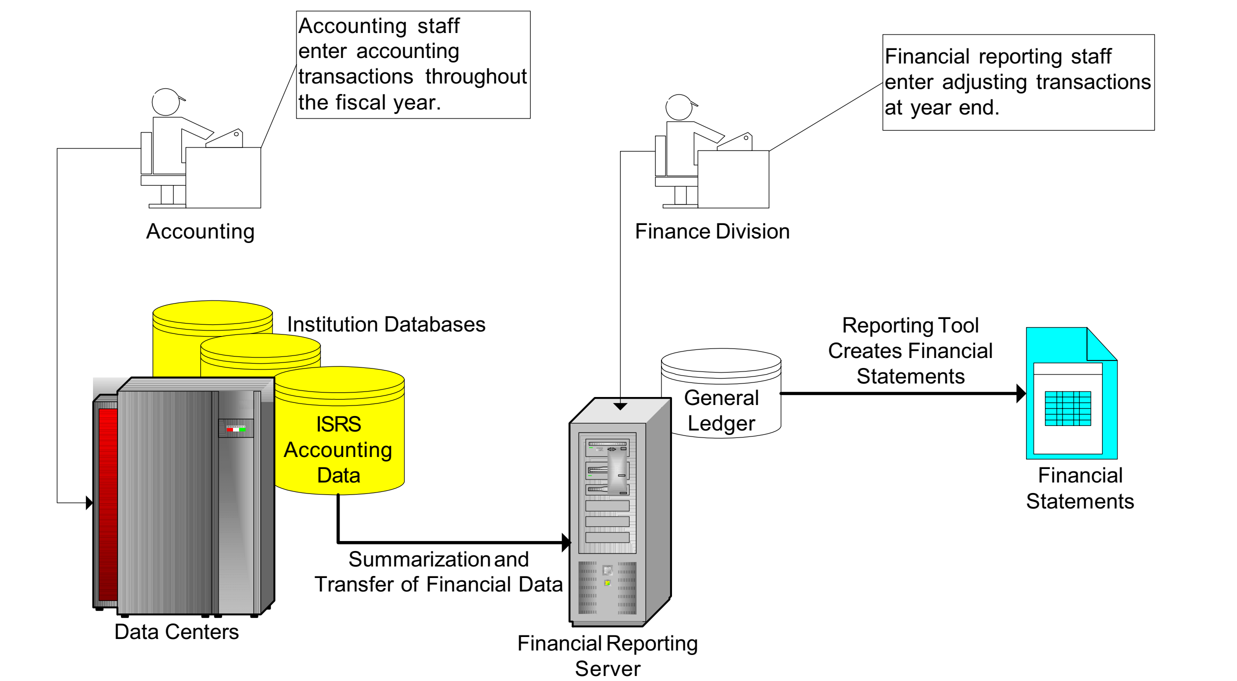
Chapter Conclusions

The Minnesota State Colleges and Universities implemented various controls to ensure the accuracy and completeness of its financial reports. However, MnSCU did not have a formal process to verify the initial entry of data summarized from it main accounting system into its financial reporting system. MnSCU also had some weaknesses in the design of its financial reporting system that allowed some data entry errors. Finally, MnSCU's list of financial reporting accounts contained many errors and inconsistencies. These weaknesses required that the financial reporting staff diligently monitor financial statement data for errors.

The foundation of MnSCU's financial reporting system was a purchased software package. This software package came standard with many computerized edits, controls, and reports. The effectiveness of these edits, controls, and reports often depended on how MnSCU had installed the software. MnSCU accountants also performed many manual procedures to ensure the accuracy of the financial statements.

Data entered MnSCU's financial reporting system either as computer-generated or people-generated transactions. To properly classify the accounting transactions into the correct institutions, funds, and reporting categories, MnSCU used an extensive list of accounts. For consistency and accuracy, MnSCU created a computer program that, three times per year, summarized financial data from its main accounting system and transferred it into the financial reporting system. This transferred data became the basis for most of the financial activities presented in MnSCU's financial statements. MnSCU's accountants adjusted the data and performed many additional reconciliations and reviews to ensure that the resulting financial data complied with accounting principles. After all the accounting transactions were entered and validated into its financial reporting system, MnSCU used a reporting tool to summarize and categorize the financial data in the financial statements. Figure 2-1 depicts this process.

Figure 2-1
MnSCU Financial Reporting System



Source: Auditor prepared.

Audit Objectives

For this audit, we designed our audit work to answer the following questions:

- Did the Minnesota State Colleges and Universities design and implement adequate controls to ensure that it properly summarized applicable accounting data from the main accounting system and transferred it into its financial reporting system?

- Did the Minnesota State Colleges and Universities design and implement specific controls within its financial reporting system to ensure that it properly transferred data to the financial statements?

To address these objectives, we interviewed information technology and business professionals who oversee the system and its controls, and used computer-assisted audit tools to test selected controls.

Current Findings and Recommendations

1. MnSCU did not have a formal process to verify the initial entry of data summarized from its main accounting system.

MnSCU did not have a formal process to verify that it properly transferred initial data summarized from its accounting system into its financial reporting system. Information technology personnel periodically ran computer programs at each college and university to summarize transactions from its main accounting system. Once summarized, an accountant transferred that data into MnSCU's financial reporting system.

Although MnSCU's procedures did not include steps for reconciliation of the data initially entered into the financial reporting system, financial reporting personnel reconciled some of the institutions to validate that the computer programs ran accurately and that the data initially transferred properly. Since the summary and transfer process runs separately for each college and university, it is important to validate the transfer of data for all institutions. COBIT standards provide that an organization should have procedures established to assure that it validates and edits input data as close to the point of origin as possible. A timely, complete reconciliation process would better ensure the detection of data errors.

MnSCU financial reporting personnel also conducted various other reconciliations throughout the financial reporting process. While those reconciliations may identify differences between MnSCU's main accounting system and the financial reporting system, they may not specifically identify that the difference resulted from inaccurate initial data transfers. Since many subsequent adjustments are based on the initial data, promptly detecting any initial data transfer errors may prevent a "ripple effect" of errors.

Recommendation

- *MnSCU should implement reconciliation steps to better validate the entry of data into the financial reporting system from the main accounting system.*

2. MnSCU's financial reporting system lacked some key edits to control data entry.

MnSCU's financial reporting system did not include edits to ensure the validity of certain transactions. While the system did ensure that all groups of transactions and funds balanced, it did not ensure that transactions balanced within institutions. The system allowed accountants to debit one institution and credit another institution, creating an imbalance. Financial reporting staff reviewed resulting financial data to determine whether imbalances existed and then processed correcting entries. For example, during fiscal year 2004, a data entry error resulted in two schools being out of balance by more than $675,000. Although MnSCU detected and corrected this error, proper system edits could have prevented the error.

MnSCU also did not activate computerized controls to validate important elements of an account. As a result, MnSCU created many accounts that had errors. MnSCU uses certain account characteristics to determine how it summarizes transactions to appear in the financial statements. When errors occur in assigning these characteristics to an account, it is possible for MnSCU's financial statements to be inaccurate. For example, MnSCU designates a fund type to categorize and report activities for its many different accounting funds. However, because of the lack of edits, accounts existed with invalid fund types. In 2004, MnSCU erroneously posted transactions to some of these accounts. Although MnSCU detected and corrected the errors, proper use of the software edits could have prevented the establishment and use of these accounts.

Recommendations

- *MnSCU should consider implementing automated controls to ensure accounting transactions balance within each institution.*

- *MnSCU should set up its financial reporting system to require and validate important data elements, such as account attributes.*

3. MnSCU did not actively monitor its list of financial reporting accounts for errors or inconsistencies.

MnSCU's financial reporting system uses an extensive list of accounts to classify accounting transactions into the correct institutions, funds, reporting categories, and object codes. MnSCU also allows each institution to define many unique account elements. These elements can make up many unique account combinations. Choosing the right account for a transaction is critical to ensure that MnSCU properly presents the financial activities in the financial statements.

During our audit, MnSCU had more than 220,000 active accounts from which to choose when posting a transaction. Many accounts were for invalid and undefined institutions, funds, and reporting categories. Numerous other accounts had inconsistencies, such as multiple fund types assigned to the same funds. In some instances, these accounts were once valid but were now obsolete; other accounts were set up in error. We estimate that over 140,000 old or erroneous accounts may exist. By actively monitoring and eliminating outdated, inactive, and erroneous accounts, MnSCU can greatly minimize the risk of fictitious transactions or errors in its financial statements.

Recommendation

- *MnSCU should routinely review its list of accounts and eliminate outdated, inactive, and erroneous accounts.*

Chapter 3. Security Controls

Chapter Conclusions

The Minnesota State Colleges and Universities generally designed and implemented controls to ensure that access to its financial reporting system was appropriately limited. However, it lacked strong password controls and did not properly limit some individuals to computer programs and data required for their normal job duties.

Maintaining adequate security controls over the financial reporting system is essential for the integrity and reliability of financial data. Although the financial reporting system does not contain confidential data or safeguard highly valuable assets, such as cash or investments, the system needs proper security controls to ensure that only authorized staff can add or edit accounts, process transactions, and modify financial statement criteria. To protect its financial reporting system, MnSCU uses many layers of security. The most critical security layers include:

- **Operating System Security.** These software packages authenticate the identity of people who try to access the computers that house the financial reporting software and its related components. They also prevent authorized individuals from accessing computer programs and data that is not required for their normal job duties.

- **Database Management System Security.** When properly configured, the database management security features prevent people from directly connecting to the database that stores financial reporting data and entering transactions without using the appropriate screens of an application.

- **Application Security.** Customizable security features within MnSCU's financial reporting software package assist in authenticating access to the application, limiting people to the specific computer screens that they need to use to fulfill their job duties, and limiting the data that a person can access.

- **Network and Perimeter Security.** MnSCU uses various firewalls and other network security components to control which computers can access the system.

Audit Objective

To assess the adequacy of these security controls, we designed our audit to answer the following question:

- Did the Minnesota State Colleges and Universities design and implement controls to ensure that access to financial reporting data and resources were appropriately limited to people who need access for their normal job duties?

To address this objective, we interviewed information technology and business professionals who oversee the system and its controls and used computer-assisted audit tools to test selected controls.

Current Findings and Recommendations

4. MnSCU lacked strong password controls for it financial reporting system.

MnSCU protects its financial reporting system at multiple levels with different security packages. Each of these security packages relies on unique user accounts and passwords to confirm the identity of persons accessing the system. However, controls used to confirm the identity of individuals were weak in several respects. Combined, these security shortcomings could jeopardize the integrity of MnSCU's financial reports.

First, MnSCU did not reasonably limit the number of invalid passwords that a person could use to try to access the financial reporting system. To reduce the risk of someone trying to guess a person's security credentials, industry best practices often suggest disabling a user account after five or fewer invalid access attempts. MnSCU's policies did not define the allowable number of invalid attempts before disabling the account.

MnSCU also did not use automated controls within some security packages to force people to change their passwords. MnSCU's policies require individuals to frequently change their passwords. Yet, without automated controls, people may not routinely change their passwords. As of April 2005, some user accounts still had the original passwords assigned by MnSCU's system administrators or the software vendors. It is especially important to immediately change default passwords because they provide an easy way to gain unauthorized access.

Finally, MnSCU did not remove some user accounts for people who no longer needed access, as required by its policies. Having unnecessary user accounts increases the risk of persons using those accounts for unauthorized access.

Recommendations

- *MnSCU should define a reasonable number of allowable passwords attempts and set up its security packages to disable accounts that exceed the threshold.*

- *MnSCU should use its security software packages to force password changes prescribed by its policies.*

- *MnSCU should promptly remove user accounts that it no longer needs.*

5. Some individuals had more access to data and system resources than was necessary.

Generally, MnSCU's multiple layers of security sufficiently limited the access of approximately 50 accountants and information technology professionals. However, many of these individuals could circumvent established controls because of weaknesses in database and file permissions. MnSCU also provided some people with access that exceeded their job duties. For example, MnSCU inadvertently gave one campus level accountant the ability to enter accounting transactions for all colleges and universities, rather than limiting that person to a specific college. In addition, a few information technology professionals inappropriately had access to enter accounting transactions and modify some computer programs.

Recommendation

- *MnSCU should ensure that it appropriately limits an individual's access to financial reporting data and resources.*

This page intentionally left blank.

Status of Prior Audit Issues
As of May 2, 2005

Most Recent Audit

Legislative Audit Report 04-39 was a follow-up audit to assess the status of various security weaknesses identified during previous information technology audits that focused on selected controls to help secure MnSCU's Integrated Statewide Records System. That report concluded that MnSCU had taken steps to resolve many of the security weaknesses reported in those prior audits, but it still lacked a comprehensive security program to effectively manage security throughout the organization.

During our current audit, we did not specifically address the status of report 04-39.

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. The process consists of an exchange of written correspondence that documents the status of audit findings. The follow-up process continues until Finance is satisfied that the issues have been resolved. It covers entities headed by gubernatorial appointees, including most state agencies, boards, commissions, and Minnesota state colleges and universities. It is not applied to audits of the University of Minnesota, any quasi-state organizations, such as metropolitan agencies or the State Agricultural Society, the state constitutional officers, or the judicial branch.

This page intentionally left blank.

Minnesota
STATE COLLEGES
& UNIVERSITIES

OFFICE OF THE CHANCELLOR
500 WELLS FARGO PLACE
30 EAST SEVENTH STREET
ST. PAUL, MN 55101-4946
ph 651.296.8012
fx 651.297.5550
www.mnscu.edu

June 20, 2005

Mr. James Nobles, Legislative Auditor
Office of the Legislative Auditor
Room 140 Centennial Building
658 Cedar Street, St Paul, MN 55155

Dear Mr. Nobles,

The purpose of this letter is to respond to the recently released audit of financial reporting Information Technology Controls for Minnesota State Colleges and Universities. As noted in the report, the audit scope was limited to selected application and security controls. We appreciate the efforts of your audit staff and the suggestions that resulted from their work.

The scope of your audit included information technology controls related to our annual financial reporting process. As an annual cycle, we have made certain cost-benefit choices regarding investment in both manual and automated controls supporting this important but somewhat ancillary reporting process. Basic cash-basis accounting data is extracted from our main accounting system and loaded into an off-line financial reporting software package. Necessary accrual accounting entries convert the basic cash-basis data to full-accrual balances following generally accepted accounting principles (GAAP). The resulting basic financial statements become part of our externally audited financial reports for the system as a consolidated whole and for twelve stand-alone colleges and universities.

The financial reporting system we use is a purchased, off the shelf product and therefore was not developed under the same security requirements or security capabilities as our MnSCU ITS developed systems. However, IT managers have taken steps to address these security issues to improve the security environment and reduce the risk of unauthorized access to this packaged product.

We believe the current financial reporting control environment, while often relying on less efficient manual control steps, is adequate and strikes a reasonable balance between costs and benefits. The fact that our externally audited financial reports have without exception received unqualified audit opinions further supports this belief. Your report concludes much the same while also stressing areas where we can either improve efficiencies or tighten controls to better limit access to the financial reporting system and the underlying data. We believe your suggested improvements are very timely and have clear value, especially as we look to expand our future financial reporting to include interim financial statements.

Our response to address the current audit findings follows.

Sincerely,

Laura M. King

Laura M. King
Vice Chancellor—Chief Financial Officer

c: James M. McCormick, Chancellor
Ken Niemi, Vice Chancellor for Information Technology & CIO

Finding 1: MnSCU did not have a formal process to verify the initial entry of data summarized from its main accounting system.

Response:

The first audit finding is an example of the trade-off between costs and benefits of automated and manual control steps. In addition to the controls mentioned in the report, Financial Reporting has implemented a detective control process of reconciling trial balance dollars from the financial reporting system back to trial balances produced by the main accounting system. This rather extensive manual reconciliation step provides assurance that the data loaded from ISRS is all inclusive. We will investigate our options for implementation of a more automated control process at the time of data transfer, such as the use of control totals. In addition, we will develop written procedures that better document existing reconciliation processes and future enhancements.

Finding 2: MnSCU's financial reporting system lacked some key edits to control data entry.

Response:

Similar to the response above for Finding 1, we have implemented manual, detective controls to assure data entry errors are discovered and corrected. This manual process is less efficient than the automated edits recommended by OLA, but the controls have proven to be effective. We will investigate OLA's suggestion of better utilizing the financial reporting system's automated editing capabilities by fund and validation of important data elements. This will require some re-engineering of how funds are defined and coded such that each fund will have to stand alone by institution, but it is again something that will be increasingly important as we move to interim fiscal year financial statements.

Finding 3: MnSCU did not actively monitor its list of financial reporting accounts for errors or inconsistencies.

Response:

We have reviewed and eliminated all erroneous accounts. Outdated and inactive accounts have been deactivated. Annually, we will review and deactivate any outdated accounts.

Finding 4: MnSCU lacked strong password controls for its financial reporting system.

Response:

The financial reporting system is a purchased system hosted by ITS and does not have the functionality to implement certain security features and functions such as strong password controls. Since MnSCU does use layers or levels of security for accessing this and other systems, the possibility of unauthorized access, while possible, is a relatively low risk.

However, to strengthen the password controls utilized on the operation of this system, the following measures have been implemented: complex password requirements have been established for the underlying Microsoft operating system; and account lockout and reset thresholds have been implemented at the operating system level. In addition, we will remove user accounts when no longer needed.

Finding 5: Some individuals had more access to data and system resources than was necessary.

Response:

> *ITS staff currently provide significant technical support for financial reporting. As part of their role in troubleshooting problems, system administrators require access to the application to work with the vendor in identifying and implementing solutions. We have carefully reviewed their access requirements and are confident that the limited number of individuals with system administration capability is essential to adequately maintain and operate the financial reporting system.*