OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Minnesota State Colleges and Universities

Information Technology Security Follow-Up

SEPTEMBER 17, 2004 **04-39**

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

Representative Tim Wilkin, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Dr. James McCormick, Chancellor
Minnesota State Colleges and Universities

Members of the Minnesota State Colleges and Universities Board of Trustees

We have conducted a follow-up audit of security concerns raised in prior Minnesota State Colleges and Universities (MnSCU) information technology audits. Our audit scope was limited to an assessment of the prior security findings. The Report Summary highlights our overall conclusions.

We decided to assess the status of prior security concerns because computer security plays a crucial role in protecting MnSCU's business systems and data. In addition, MnSCU's systems are in a constant state of change due to upgrading and refinement.

We conducted our audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of management controls relevant to the audit objectives. We obtained our evaluation criteria from several sources, including the *Control Objectives for Information and Related Technologies (COBIT)* and publications provided by hardware and software manufacturers whose products are used by MnSCU.

To meet the audit objectives, we interviewed the MnSCU information technology professionals who are responsible for security controls. In addition, we analyzed security data from the operating system and database management system underlying MnSCU's business systems.

Information technology audits frequently include a review of sensitive security data that is legally classified as nonpublic under the Minnesota Data Practices Act. In some cases, to protect state resources and comply with the Minnesota Data Practices Act, we must withhold security-related details from our publicly released report. When these situations occur, we communicate all pertinent details to agency leaders in a separate, confidential document. For this audit, we issued a separate, confidential document to the management of the Minnesota State Universities and Colleges.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: July 30, 2004

Report Signed On: September 14, 2004

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
Information Technology Security Follow-Up

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
Neal Dawson, CPA, CISA	Information Technology Auditor

Exit Conference

We discussed the results of the audit with the following representatives of the Minnesota State Colleges and Universities at an exit conference on September 7, 2004:

Laura King	Vice Chancellor and Chief Financial Officer
Ken Niemi	Vice Chancellor and Chief Information Officer
Joanne Chabot	Deputy Chief Information Officer
John Asmussen	Executive Director – Internal Auditing
Beth Buse	Deputy Director – Internal Auditing

Minnesota State Colleges and Universities
Information Technology Security Follow-Up

Report Summary

Key Conclusion:

MnSCU has taken steps to resolve many of the security weaknesses reported in prior audits; however, it has not developed a comprehensive security program to effectively manage security throughout the organization. Furthermore, we question whether MnSCU can develop a successful security program given the limited resources currently devoted to security.

Finding:

- MnSCU has not resolved some outstanding security weaknesses, nor has it developed a comprehensive security program. (Finding 1, page 7)

Audit Scope:

Audit Period:
As of July 2004

Selected Audit Areas:

- Prior audit findings on computer security

Background:

We have performed several information technology audits at MnSCU since 1996. These audits typically focused on selected "general controls" that help secure its Integrated Statewide Records System (ISRS). These audits found similar and often serious security concerns.

The purpose of this information technology audit was to assess and report the status of security weaknesses described in prior audit reports. We limited our scope to those weaknesses that impacted ISRS.

This page intentionally left blank.

Chapter 1. Introduction

The purpose of this information technology audit was to assess and report the status of selected security-related weaknesses described in prior audit reports. We have performed several information technology audits at MnSCU since 1996. These audits typically focused on "general controls." General controls are not unique to specific computerized business systems; rather, they apply to all business systems that operate in a particular computing environment. Examples of general controls include computer security policies, procedures, and standards.

Prior to 2004, our audits focused on general controls that help secure MnSCU's primary business system, the Integrated Statewide Records System (ISRS). Our audits found similar and often serious security weaknesses. For the first time in 2004, we performed audits of three other computer applications. They included MnSCU's Data Warehouse, the Degree Audit Reporting System (DARS), and the Course Applicability System (CAS). These audits also encountered similar security concerns.

MnSCU is an extremely complex organization from both a business and technological perspective. One thing that leads to its complexity is the size and diversity of the organization. It consists of the Office of the Chancellor, 5 community colleges, 8 technical colleges, 12 combined community and technical colleges, and 7 state universities. These colleges and universities are located on 53 campuses throughout the state, annually serving over 165,000 students in credit courses and 240,000 students in noncredit courses. MnSCU employs approximately 16,000 people (full year equivalent) and has an operating budget that exceeds $1.6 billion.

Technologically, MnSCU is also extremely large and diverse. Staff indicated that the organization likely has over 50,000 computers. While individual colleges are responsible for managing many of those computers, the Office of the Chancellor manages the critical system-wide business systems. For example, it developed ISRS to help institutions manage many of its business activities. ISRS consists of over 20 modules, including accounting, human resources, purchasing, student registration, accounts receivable, and financial aid. The Office of the Chancellor manages an ISRS database for each institution. Collectively, these databases store about 700 million rows of data. The Office of the Chancellor also manages several other mission critical business systems, including a data warehouse, an instructional management system, and others. To support its systems, the Office of the Chancellor manages a large computer network consisting of over 100 servers, 50 firewalls, 70 routers, and many other devices.

Security over many of these computer systems is vital in ensuring:

- Systems are available for use by staff and students.
- Information maintained in these systems is both complete and accurate.
- Confidential data is protected from unauthorized disclosure.

This page intentionally left blank.

Chapter 2. Security Follow-up

Chapter Conclusions

MnSCU has taken steps to resolve many of the security weaknesses we reported during prior audits. Although progress has been made, continued work is necessary to fully resolve several of the weaknesses. Of most significance is that MnSCU has not developed a comprehensive security program to effectively manage security risks throughout the organization. Furthermore, we question whether MnSCU can develop a successful security program given the resources currently devoted to security.

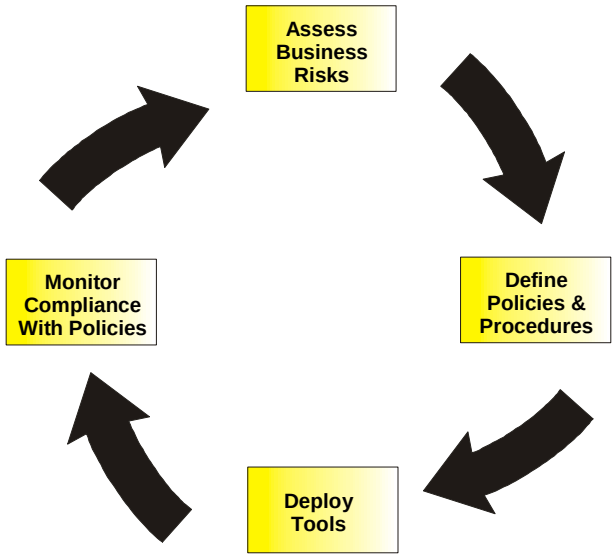
Audit Objective

We designed our work to evaluate and report the status of selected security- related audit findings cited in prior reports issued by the Office of the Legislative Auditor.

Background

Every organization needs strong security controls to protect its critical computer systems and 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. 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

Figure 2-1
The Ongoing Security Management Lifecycle



Source: Auditor prepared.

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 after a violation has been detected or an audit finding has been reported.

Status of Prior Audit Findings

Table 2-1
Assessment of Prior Security-Related Findings

Finding Statement	Audit Report Number	Status Assessment	Comment
MnSCU has not implemented a fully effective security infrastructure.	00-53	Partially Resolved	Although MnSCU has made improvements to address security issues, it has struggled to develop a comprehensive security program. We do not believe it can develop a comprehensive program given the limited resources currently devoted to security matters.
MnSCU has not implemented formal standards and procedures for granting access to its information technology professionals and software.	03-33	Resolved	MnSCU placed people into groups or roles based upon job duties. Based on these roles, it defined the levels of access appropriate for each group and implemented the desired access. MnSCU also implemented a process to identify any users that had access that deviated from the defined role.
Many information technology professionals have unnecessary system privileges, and an excessive number are authorized to enter security transactions.	03-33	Substantially Resolved	MnSCU has made significant improvements in this area; however, some people continue to have unnecessary system privileges and too many are authorized to enter security transactions.
Some computer programs, including SCUPPS programs, are not properly or consistently secured.	03-33	Partially Resolved	MnSCU made some security improvements but did not develop and implement standards for securing critical programs.
Several users can view, alter, or delete critical data from uncontrolled environments.	03-33	Substantially Resolved	MnSCU revoked this access for many of the people that did not need it; however, we still found some examples that had not been resolved.
MnSCU did not enforce strong password management controls.	03-33	Partially Resolved	MnSCU resolved several of the password-related weaknesses; however, others persist.

Finding Statement	Audit Report Number	Status Assessment	Comment
MnSCU does not have effective monitoring of security-related events.	03-33	Partially Resolved	MnSCU implemented procedures to monitor and review certain operating system security events. We believe MnSCU should also consider monitoring other risky events and assess its database monitoring needs.
Some interface files were not appropriately secured during transmission.	03 -33	Resolved	MnSCU implemented technologies to properly encrypt the interface files.

Current Finding and Recommendations

1. MnSCU has not fully resolved some outstanding security weaknesses, nor has it developed a comprehensive security program.

Although, as shown in Table 2-1, MnSCU made progress in resolving many of the prior security-related audit findings, several remain partially unresolved. Of most significance, MnSCU has not developed a comprehensive security program to effectively manage security risks throughout the organization. To be successful, an organization must have a security program made up of many components, including a periodic risk assessment and the development of policies and detailed procedures that describe how to mitigate specific risks. In addition, a security program must include monitoring procedures to validate the effectiveness of its security controls. Without these and other components, an organization cannot effectively manage the security risks.

We think it will be unlikely, if not impossible, for MnSCU to develop a comprehensive security program given the current level of staff resources devoted to security. Although MnSCU has created a Security Office, it consists of only two staff. In addition, its director has other responsibilities besides security, and the second staff member manages user accounts. As a result, security efforts have been primarily reactive rather than proactive. The Security Office has relied heavily upon other information technology professionals within the organization to make security decisions and help implement security measures. Although these professionals and others play a vital role in security, such heavy reliance on them typically does not work well over time because they are too busy performing their day-to-day responsibilities. Furthermore, technology and related risks are constantly changing; therefore, it is critical that MnSCU have professionals whose job responsibilities are devoted to managing security.

MnSCU is not unlike many large organizations. Our audits of other large state agencies often find similar weaknesses, including the lack of an overall strategy to effectively manage security risks. Without adequate staffing and a comprehensive security strategy, MnSCU will be unable to successfully manage security throughout its organization. As a result, there may be a negative impact on computer systems availability, data integrity, or data confidentiality.

Recommendations

- *MnSCU should continue its efforts to resolve prior computer security findings.*

- *MnSCU should develop a comprehensive security program to effectively manage security risks throughout the organization. Furthermore, it should assess its current and future security needs to ensure resources are adequate to provide for an effective security program.*

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

September 14, 2004

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

Dear Mr. Nobles,

We appreciate the objective review the Office of the Legislative Auditor has made of our efforts to improve our overall security environment at the Minnesota State Colleges & Universities, and particularly your recognition of the significant progress we have made in resolving your previous findings despite limited resources available. We are satisfied that we have made much progress, and that more work will always need to be done. The relatively broad scope of some previous findings makes it extremely difficult to state that they have been fully resolved, but we will continue our efforts to make that happen.

We believe that the significant progress to date in improving our technical security environment has positioned us to now focus on the broader, organization-wide effort to establish a comprehensive security program, a program which will move beyond the mere technical aspects of security implementation. Over the next year, we intend to plan and begin implementation of a comprehensive security program, as recommended by your current Follow-up Audit. Of course, the current fiscal environment makes it extremely difficult to identify and earmark financial and human resources needed for such a comprehensive program. We will, therefore, carefully assess our current investments in security and develop a creative and innovative plan to enable us to upgrade our current investments in this area.

Thank you again for recognizing our progress in improving the security environment within the Minnesota State Colleges & Universities, and for your ongoing support in this long-term effort.

/s/ Kenneth F. Niemi

Kenneth F. Niemi
Vice Chancellor for Information Technology

/s/ Laura M. King

Laura M. King
Vice Chancellor – Chief Financial Officer

c: James H. McCormick, Chancellor