OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Minnesota State Colleges and Universities
Systemwide Access to MnSCU Data

NOVEMBER 22, 2000 00-53

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

OLA

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

Representative Dan McElroy, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Morrie J. Anderson, Chancellor
Minnesota State Colleges and Universities

Members of the Minnesota State Colleges and Universities Board of Trustees

We have conducted a financial-related audit of selected areas related to security over the Minnesota State Colleges and Universities' (MNSCU) computing environment, as further explained in Chapter 1. We emphasize that this has not been a complete audit of all MnSCU computer systems or data centers. Our audit focused on employees with extremely powerful security clearances to MnSCU's computing environment. The Report Summary highlights the audit objectives and conclusions. We discuss these issues more fully in Chapter 2.

We conducted our audit in accordance with *Government Auditing Standards*, as issued by the Comptroller General of the United States. These standards require that we obtain an understanding of management controls relevant to the audit. The standards also require that we design the audit to provide reasonable assurance that the college complied with the provisions of laws, regulations, contracts, and grants significant to the audit. The management of the college is responsible for establishing and maintaining the internal control structure and for compliance with applicable laws, regulations, contracts, and grants.

This report is intended for the information of the Legislative Audit Commission and the management of MnSCU. This restriction is not intended to limit the distribution of this report, which was released as a public document on November 22, 2000.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: September 22, 2000

Report Signed On: November 16, 2000

Minnesota State Colleges and Universities
Systemwide Access to MnSCU Data

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

Exit Conference

We discussed the findings and recommendations with the following representatives of the Minnesota State Colleges and Universities at the exit conference held on November 7, 2000:

Ken Niemi	Chief Information Officer
Dale Jarrell	Chief Technology Officer
Larry Simmons	System Director, Office of Security
John Asmussen	Executive Director, Office of Internal Audit
Beth Buse	Deputy Director, Office of Internal Audit

Minnesota State Colleges and Universities System
Systemwide Access to MnSCU Data

Report Summary

This is our second security-related audit of MnSCU's information systems. The first audit, performed in June 1997, concluded, "Every institution's critical business data is at risk because MnSCU data centers have serious security weaknesses."

Our current audit focused on employees with extremely powerful security clearances to the Minnesota State Colleges and Universities (MnSCU) computing environment. In an appropriately controlled environment, extremely powerful security clearances are typically limited to certain information technology professionals who manage the computerized infrastructure.

Key Audit Conclusions:

MnSCU's critical business data continues to be at risk because it has not formally defined its security infrastructure. More specifically:

- MnSCU has not conducted a formal risk assessment to identify vulnerabilities in its business systems. In addition, MnSCU does not have written security policies and procedures to control and monitor people with extremely powerful security clearances. (Finding 1, page 6)

Though MnSCU made progress resolving some of the weaknesses identified in the prior audit, it cannot effectively manage its information security risks until it formally defines its security infrastructure. Without policies, MnSCU cannot effectively deploy security administration tools. Challenging the appropriateness of employee security clearances is also difficult without written policies. Many employees who we identified with excessive security clearances were not challenged by MnSCU's Office of Security.

We also question the sufficiency of MnSCU's security resources. For example, the Office of Security employs only two staff, one of whom also oversees all software development for MnSCU.

Chapter 1. Introduction

This audit focused on employees with extremely powerful security clearances to the Minnesota State Colleges and Universities (MnSCU) computing environment. In an appropriately controlled environment, extremely powerful security clearances are typically limited to certain information technology professionals who manage the computerized infrastructure.

MnSCU consists of 35 different higher education institutions with 53 campus locations. It serves approximately 230,000 students in for-credit courses[1]. An internal audit identified that 135,000 students and 4,000 businesses were served in customized training programs and 89,000 students in non-credit continuing education programs. For fiscal year 2000, MnSCU budgeted total revenues of $1.3 billion from state appropriations, tuition and fees, federal and state financial aid, and other sources. MnSCU planned total operating costs of approximately $1.1 billion for fiscal year 2000.

MnSCU has developed a collection of computer systems, or modules, to help institutions manage their business activities. This system, referred to as the Integrated Statewide Records System (ISRS), consists of over 20 modules, including accounting, human resources, purchasing, registration, accounts receivable, and financial aid.

Each institution stores its business data in its own database. MnSCU houses each institutional database at one of four regional data centers and connects them to the central computer at that site. This connection and the State of Minnesota's wide area network give campus staff instantaneous access to their business data. MnSCU also makes an exact copy of each institution's database. This copy, referred to as an institution's replicated database, gives staff a tool for ad-hoc reporting.

Table 1-1 shows the location of each data center, the number of MnSCU databases served, and the total number of users.

Table 1-1
Total Number of Databases and Users Served By Each MnSCU Data Center
As of August, 2000

Data Center Location	Total Number of Databases	Total Number of Users
Minnesota State University Moorhead	11	1,189
St. Cloud State University	7	1,448
Minnesota State University, Mankato	8	1,451
Metro Regional Computing Center (St. Paul, MN)	13	1,664
Total	39	5,752

Source: Security data provided by MnSCU information system personnel.

MnSCU institutions are highly reliant on the integrity of the data in each institutional database. Accordingly, strong controls are imperative to ensure data is both accurate and complete.

Minnesota State Colleges and Universities System
Systemwide Access to MnSCU Data

Information security relies highly on MnSCU's ability to secure its data through various access control methods. MnSCU uses security software to limit user access to the various ISRS modules and the underlying institutional databases. However, by itself, specialized software cannot protect data from unauthorized use, modification, or destruction. Policies, standards, and procedures for system users are also necessary.

MnSCU's computing environment is very complex. To improve management of the environment and its information security structure, MnSCU recently completed a reorganization of its information technology department. It also created the Office of Security and charged it with responsibility for developing, implementing, and monitoring systemwide compliance with security policies, standards, and procedures.

This is our second security-related audit examining MnSCU information system security. The first audit in July 1997 reported seven serious security weaknesses over MnSCU's computerized business systems. MnSCU made progress on these audit findings; however, it has not resolved the underlying problem as discussed in Finding 1 of this report.

Chapter 2 discusses the scope of our current security audit and the conclusions that we reached.

Chapter 2. Systemwide Access to MnSCU Data

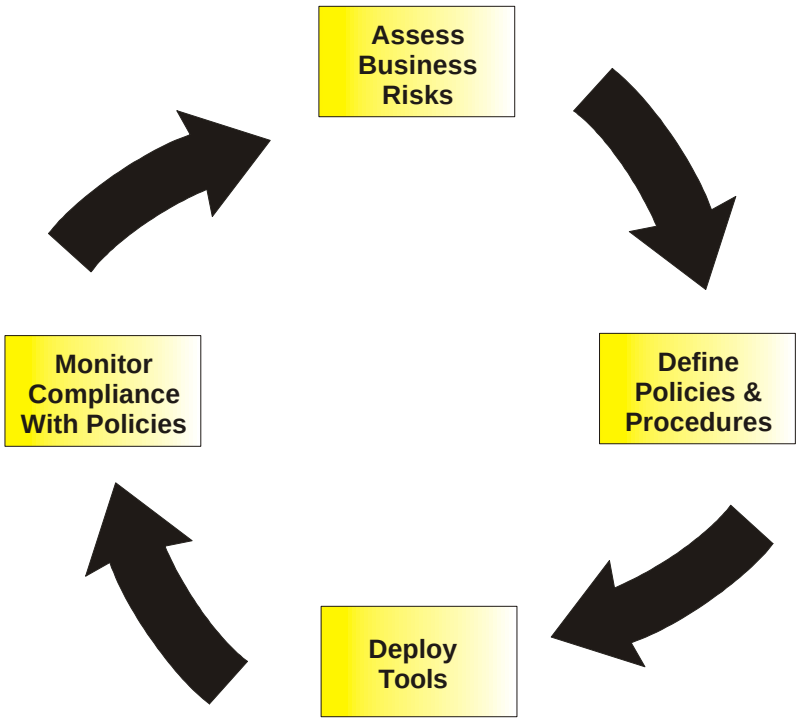
Chapter Conclusions

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. MnSCU has not conducted a formal risk assessment to identify vulnerabilities in its computerized business systems. In addition, MnSCU does not have written security policies and procedures to control and monitor staff who have extremely powerful security clearances. Without policies, MnSCU cannot effectively deploy security administration tools nor challenge the appropriateness of employee security clearances. Many employees who we identified as having excessive security clearances were not challenged by MnSCU's Office of Security.

We also question the sufficiency of MnSCU's security resources. For example, the Office of Security has only two employees, one of whom also oversees all software development efforts for MnSCU.

Managing security over a computerized information system is an ongoing process. As depicted in Figure 2-1, this process begins with a formal risk assessment. This risk assessment process helps an organization inventory its critical business data by determining the impact if data is lost, inappropriately modified, or disclosed to unauthorized people. Once complete, an organization can define policies and procedures to effectively mitigate its' risks. Next, the process requires the deployment of tools, including security software, to enforce the organization's policies. Finally, periodic monitoring helps an organization evaluate both compliance and the effectiveness of its policies and procedures. 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. The Office of Security is responsible for developing and implementing MnSCU's information security program.

Figure 2-1
Security Management Lifecycle



Source: Auditor prepared.

MnSCU utilizes security software to authenticate users and limit the electronic resources they can access and the actions they can execute. With this software, people can be granted powerful clearances to systemwide data and resources. Some people are granted "privileges". The most powerful privileges are those that allow the user to bypass security, giving them unfettered access to data and resources.

Audit Objective and Methodology

We focused our audit of MnSCU security on the following objective:

- Does MnSCU limit systemwide access to computer system resources and data to only those employees who need such clearances to fulfill their job responsibilities?

To address this objective, we reviewed MnSCU's system security controls, interviewed information technology personnel, and analyzed an extensive amount of electronic security data from each of the four data centers.

Conclusions

Every campus' critical business data is at risk because MnSCU does not have an effective security infrastructure ensuring access to system resources and data is sufficiently restricted. MnSCU has not conducted a formal risk assessment to identify vulnerabilities in its business systems. MnSCU also does not have written security policies and procedures to control and monitor employees who have extremely powerful security clearances. Without policies, MnSCU cannot effectively deploy security administration tools. Challenging the appropriateness of employee security clearances is also difficult without written policies. Many employees who we identified as having excessive security clearances were not challenged by MnSCU's Office of Security. We also question the sufficiency of MnSCU's security resources. For example, the Office of Security has only two employees, one of whom also oversees all software development efforts for MnSCU.

1. MnSCU has not implemented a fully effective security infrastructure.

MnSCU has not completed a formal information security risk assessment. Without a complete assessment of its risks, MnSCU cannot determine what policies and procedures are needed. Furthermore, it cannot implement an effective security program to periodically monitor both compliance with and the effectiveness of its policies. As a result, some employees may have excessive access. Finally, we question whether MnSCU's current resources are sufficient to implement and sustain an effective security infrastructure.

MnSCU has implemented some basic security policies, however, additional policies are needed. For example:

- MnSCU has not defined which employees have the authority to enter security transactions. This is critical since many users currently have the ability to enter transactions that modify the data used by the security software to determine whether users obtain system access.

- MnSCU has not required documentation, including proper management authorizations and statements of need, to create or modify accounts with powerful clearances. In addition, it does not have a policy and procedure to periodically reauthorize powerful accounts. As a result, it is difficult for the security function to challenge the appropriateness of these powerful accounts.

MnSCU has not implemented an effective program for testing and evaluating security, including any controls that have been implemented. For example, it has not defined the transactions or events, including the use of powerful accounts, that the Office of Security should monitor. In fact, the security staff were unfamiliar with the tools available for monitoring security.

We analyzed MnSCU's most powerful accounts and found:

- Each data center has between 34 and 36 accounts that have been granted one or more powerful operating system privileges, and between 9 and 12 accounts that have been

granted powerful database management system privileges that give staff the ability to bypass security.

- Five software development staff held powerful privileges. As a result, unauthorized or erroneous computer program code software could be introduced to MnSCU's computing environment. Also, two college employees held powerful privileges even though MnSCU's data centers are managed by system office staff. Accordingly, college employees should not have powerful clearances to systemwide resources.

- Access was not always consistent across the four regional data centers, suggesting that other people may have excessive access to MnSCU's computing environment. For example, staff who performed the same functions at multiple data centers did not always have consistent access at each data center. Also, similar positions at different data centers often held different clearances. In some cases, staff had powerful clearances at data centers where they do not work.

- MnSCU did not properly secure a computer program that is used to create and modify accounts. To run the program, information technology staff must have a powerful privilege. The privilege granted them with greater access than is needed to complete their job responsibilities.

- 50 people, including at least five college employees, were granted explicit clearances that gave them the ability to alter or delete data from uncontrolled environments. We believe the majority of these people do not require this access to these systems.

Finally, we question whether MnSCU's current resources are sufficient to implement and sustain an effective security infrastructure. The Office of Security consists of only two staff: its director and a security administrator. Currently, its director also serves as MnSCU's director of software development. As a result, the position spends less than full time on security-related matters. To make the situation more difficult, the security staff need additional training on how to use MnSCU's operating system, and other software or tools, to protect and monitor access to its data and resources.

Recommendations

- *MnSCU should complete an assessment of its security-related risks and develop additional security policies and procedures to address these risks.*

- *MnSCU should effectively deploy security administration tools and provide for a process to challenge the appropriateness of employee security clearances.*

- *MnSCU should implement a program to periodically test and evaluate the effectiveness of any system security controls being relied upon.*

- *MnSCU should determine whether its resources are adequate to implement and sustain an effective security program.*

Status of Prior Audit Issues
As of September, 2000

Most Recent Audits

Other Information System Security Audits

Legislative Audit Report 97-46, issued in August 1997, examined MnSCU information system security as of June 1997. The audit raised seven serious audit findings related to security concerns over MnSCU's computerized business systems. Progress on the audit findings were monitored by MnSCU's Office of Internal Auditing and a follow-up report issued in March 1998. Our current audit did not include a complete follow-up of these prior findings, but included a focused review of powerful system clearances held by information technology professionals who manage MnSCU's computer resources and data. We found that MnSCU's critical business data continues to be at risk because it does not have an effective security infrastructure, as discussed in Finding 1 of 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. However, Finance has delegated this responsibility for audits of the Minnesota State Colleges and Universities (MnSCU) to the MnSCU Office of Internal Auditing. MnSCU's Office of Internal Auditing 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. The process covers all colleges and universities within the MnSCU system.

System Access to MnSCU Data
Office of the Legislative Auditor
November 15, 2000

MnSCU System Office Response:

We agree with the general recommendations listed on page 7. Many of these issues were in the process of resolution during the audit, and the Audit Committee of the MnSCU Board of Trustees was briefed on MnSCU Information Technology Services security plans and implementation during their October meeting.

In response to the specific recommendation on MnSCU's allocation of security resources, before this audit MnSCU had implemented the plan to build an Information System Security Office starting with three staff positions. As we develop the Office staff and implement the Security Program as planned, we will continually evaluate the Security Office staffing requirements and add resources as needed. A formal security risk assessment will be completed with the objectives of identifying threats, vulnerabilities, and recommended countermeasures. The levels of risk acceptable to management and the countermeasures implemented will significantly determine the long-term security staffing requirements. In addition, the information security responsibilities delegated to MnSCU's institutions will be a determining factor in the central staffing needs. The distributed information security responsibilities will be an essential policy recommendation from the Information Security Steering Committee to MnSCU management.

Response to specific findings:

1. MnSCU has not performed a formal risk assessment
   A security risk assessment is being planned as part of the Information Security Program Development Plan of the Security Office.
   Planned Completion Date……..March 2001
   Assigned to ……Larry Simmons; Project Manager

2. MnSCU has not defined which people have the authority to enter security transactions.
   There is a procedure being used it but has not been formally documented. A documented procedure will be established.
   Planned completion date……December 11, 2000
   Assigned to ……Bill Russ

3. MnSCU does not have a formal process to grant or revoke security clearances for its IT professionals.

   There is a procedure being used but it has not been formally documented. A documented procedure will be established.
   Planned completion date……December 11, 2000
   Assigned to ……Bill Russ

4. Each data center has between 34 and 36 accounts that have been granted one or more powerful Open VMS privileges that give the user the ability to bypass security system-wide. Some of these people may not need this access to fulfill their daily job functions.

   Through the elimination of unnecessary privileges that are no longer needed (that were needed during ISRS development) and the establishment of limited privileges based on more current and precise job responsibilities, a uniform use of privileges across data centers will be established. Procedures for maintaining the granting of these procedures will be established.
   Planned completion date……December 11, 2000
   Assigned to ……Bill Russ

5. Each data center has between 9 and 12 accounts that have been granted identifiers that hold powerful Oracle Rdb privileges, giving the user the ability to perform any data definition or data manipulation operation, or modify security on any table or database. Some of these people may not need these privileges to perform their daily job function.

   A uniform use of privileges across data centers will be established. Procedures for maintaining the granting of these procedures will be established based on more current and precise job responsibilities.
   Planned completion date……December 11, 2000
   Assigned to ……Bill Russ

6. Some users have inappropriate access through SQL services.

   Users will be sent a letter notifying them that their accounts are being terminated and that they need to reapply for the access rights. Rights will be granted on the basis of the specific job needs, as based on established procedures.
   Planned completion date……December 11, 2000
   Assigned to ……Bill Russ

Data source: NiemiK11/15/00 12:05:47 PM

/s/ Morrie Anderson