O L A

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Minnesota State Colleges and Universities
Degree Audit Reporting and Course Applicability Systems
Information Technology Audit

JULY 15, 2004 **04-28**

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 an information technology audit of selected components of the Degree Audit Reporting (DARS) and Course Applicability (CAS) Systems currently used by the Minnesota State Colleges and Universities (MnSCU). Our audit scope was limited to security and application controls. The Report Summary highlights our overall audit conclusions. The specific audit objectives and conclusions are contained in the individual chapters of this report.

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 to support DARS and CAS.

We selected DARS and CAS for audit based on a number of factors such as newly implemented applications, sensitive student data, and agency input. To meet the audit objectives, we interviewed the information technology and business professionals at MnSCU who managed the systems and designed its controls. We also used computer-assisted audit and vulnerability assessment tools to test critical controls in the DARS, CAS, computer operating systems, and database management 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 Colleges and Universities.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: June 1, 2004

Report Signed On: July 12, 2004

Minnesota State Colleges and Universities
Degree Audit Reporting and Course Applicability Systems
Information Technology Audit

Table of Contents

Audit Participation

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

Claudia Gudvangen, CPA	Deputy Legislative Auditor
David Poliseno, CPA, CISA	Audit Manager
Eric Wion, CPA, CISA	Auditor-in-Charge
Neal Dawson, CPA, CISA	Information Technology Auditor
Scott Tjomsland, CPA	Team Leader
Sally Tefera	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 June 22, 2004:

Laura King	Vice Chancellor and Chief Financial Officer
Ken Niemi	Vice Chancellor – Chief Information Officer
Gary Langer	Vice Chancellor for Academic Programs
Joanne Chabot	Deputy Chief Information Officer
Bev Shuft	Security Director
John Asmussen	Executive Director – Internal Auditing
Beth Buse	Deputy Director – Internal Auditing

Minnesota State Colleges and Universities
Degree Audit Reporting and Course Applicability Systems
Information Technology Audit

Report Summary

Key Conclusion:

The Minnesota State Colleges and Universities (MnSCU) designed adequate application controls to help ensure that the Degree Audit Reporting System (DARS) and the Course Applicability System (CAS) properly processed transactions. It did not, however, design and implement adequate security controls to protect the integrity and confidentiality of its DARS and CAS data.

Findings:

- MnSCU did not design and implement an effective security infrastructure for DARS and CAS. (Finding 1, page 6)
- DARS allowed users to view, alter, or delete data from uncontrolled environments. (Finding 2, page 7)
- Several people and software accounts had unnecessary access to DARS and CAS. (Finding 3, page 7)
- Controls used to confirm the identity of CAS users were weak. (Finding 4, page 8)
- MnSCU did not remove unnecessary and insecure services from its CAS server or perform important system maintenance procedures in a timely manner. (Finding 5, page 9)
- DARS and CAS were not adequately monitored for unauthorized or inappropriate attempts. (Finding 6, page 10)

The audit report contained six findings relating to computer security weaknesses.

Audit Scope:

Audit Period:
As of May 2004

Selected Audit Areas:

- Security Controls
- Application Controls

Background:

DARS and CAS are commercial software applications purchased by MnSCU.

DARS is used to define the requirements for every degree offered. It can be used to help students plan and monitor their academic progress. College employees also use it to ensure students meet graduation requirements. Each of MnSCU's 32 institutions has its own DARS database.

CAS is a web-based system that allows anyone with access to the Internet to research the degrees offered by each MnSCU institution as well as the requirements for them. Also, students can identify courses that transfer from one institution to another. Each of MnSCU's institutions shares a single CAS database. As of the time of our audit, nine of MnSCU's institutions had implemented CAS.

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) Degree Audit Reporting System (DARS) and Course Applicability System (CAS). Both systems are commercial software applications that were purchased by MnSCU. 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 data.

<u>DARS</u>

DARS is a computer-based system used by MnSCU's 32 institutions to define the requirements for every education program or degree they offer. The system helps students plan and monitor their progress toward achieving a degree by identifying:

- all the requirements needed to complete a program or degree;
- the courses already completed, including accepted transfer courses, and how they pertain to the program's requirements; and
- the remaining requirements and the courses that would satisfy those requirements.

DARS also assists student advisors registrar staff who process student graduation requests.

Each institution stores its DARS data in its own database at one of four MnSCU data centers located throughout the state. DARS obtains some student-related information, such as courses taken, from MnSCU's Integrated Statewide Records System (ISRS).

<u>CAS</u>

CAS is a web-based computer system that will be used by each MnSCU institution. At the time of our audit, the system had been implemented by nine of MnSCU's institutions. The system allows anyone with access to the Internet to research the programs or degrees offered by each MnSCU institution as well as the requirements for them. Also, the system can be used to identify the courses that transfer from one college to another. Students that are contemplating a transfer can self-report the courses they have already taken and submit that coursework to any institution for evaluation against that institution's academic programs. Although the functionality exists for students to electronically import course work from ISRS, MnSCU has not implemented this feature.

Unlike DARS, each institution does not have its own CAS database. Instead, MnSCU maintains a single CAS database. Each institution is responsible to process and update its own CAS information. MnSCU extracts certain data, including program degree requirements and course transfer rules, from each institution's DARS database and loads it into CAS.

Security and application controls are important because students and MnSCU employees use the systems to make important decisions. Also, these systems contain confidential student data.

Chapter 2. Security and Application Controls

Chapter Conclusions

MnSCU designed adequate application controls to help ensure DARS and CAS properly processed transactions. It did not, however, design and implement adequate security controls to protect the integrity and confidentiality of its DARS and CAS data. Generally, MnSCU did not design and implement an effective security infrastructure for these systems. These security shortcomings are addressed in seven detailed audit findings.

Audit Objectives

This information technology audit assessed the adequacy of selected DARS and CAS general and application controls. Specifically, we designed our work to answer the following questions:

- Did MnSCU design and implement general security controls to protect the integrity and confidentiality of critical DARS and CAS data?

- Were application controls sufficient to ensure DARS and CAS properly processed transactions?

Background

Generally, three security software packages work together to protect critical DARS and CAS 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 helps prevent unauthorized people from accessing the database and critical programs that underlie MnSCU's business systems, including DARS and CAS. 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 helps restrict people's access to data based upon job duties. In addition, it can be configured to help prevent people from directly connecting to the database, effectively bypassing DARS or CAS screens. The Office of the Chancellor also is responsible for implementing and maintaining database management system security.

- **Application Security.** Vendor defined security groups within CAS limit people to the specific web pages and functions that they need to fulfill their job duties. DARS does not utilize application level security. Instead, database security limits what people can and cannot do. Each institution is responsible for determining the security needs of its systems' users.

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.

In addition to properly securing systems, it is important to implement good application controls. When practical, computerized application controls are preferred over manual controls because computerized controls are applied more consistently and accurately. Application controls can be preventative or detective in nature. Generally, preventative controls are desired because they stop invalid data or transactions from occurring. Detective controls, on the other hand, are applied after-the-fact.

Findings and Recommendations

1. MnSCU did not design and implement an effective security infrastructure for DARS and CAS.

Although MnSCU deployed several security tools to protect DARS and CAS data, shortcomings in other aspects of its security program diminished the effectiveness of these tools.

- MnSCU did not formalize detailed standards and procedures for configuring, managing, and securing DARS and CAS systems. Defining and documenting this information is vital because it provides security professionals with criteria to configure security tools and make consistent security decisions. Documentation also helps ensure the continued understanding and operation of critical security controls, should key employees leave the organization.

- MnSCU did not designate any information technology professionals to actively manage and secure the server CAS runs on. This is important because software must be updated in a timely manner when security flaws are discovered and servers must be monitored on an ongoing basis for unauthorized access attempts or other security violations.

- MnSCU did not periodically test its servers for exploits or changes and then compare the results to documented standards or baseline configurations.

- MnSCU designated a single person to perform several critical and incompatible duties. This individual developed, tested, and ran some programs and also performed duties that are typically associated with a database administrator.

Recommendations

- *MnSCU should develop detailed standards and procedures for configuring, managing, and securing its DARS and CAS-related systems.*
- *MnSCU should designate information technology professionals to actively manage the CAS server.*
- *MnSCU should periodically test its servers and validate the adequacy of its controls.*
- *MnSCU should adequately separate critical and incompatible duties.*

2. DARS allows users to view, alter, or delete data from uncontrolled environments.

Generally, MnSCU employees view, alter, or delete DARS data by using the pre-designed application screens. These screens contain edits that are extremely important because they protect the integrity of data that flows into each institution's database. Unfortunately, due to a poor system design, DARS allowed any user to view and potentially update or delete data directly in each database without using the appropriate screens. We believe this serious security weakness should have been resolved before purchasing and implementing DARS.

Recommendation

- *MnSCU should work with the DARS vendor to resolve this security weakness or devise alternative controls to limit who can bypass DARS screens and interact directly with each institution's database.*

3. Several accounts had excessive clearance to the DARS and CAS related systems.

During our audit, we identified several people with excessive security clearances not needed to fulfill their job duties. In addition, some accounts used by software products had been assigned unnecessary and very powerful clearances. In some cases, MnSCU simply assigned these accounts too much access. However, in other cases, the accounts were unintentionally granted excessive access due to certain misconfigured security settings. For example, one misconfigured security setting resulted in hundreds of unauthorized people having the ability to view any DARS data, including some confidential data. To prevent unauthorized changes or disclosure of confidential information, the access granted to accounts must be limited to what is needed.

Recommendation

- *MnSCU should examine security settings and review security clearances to ensure the access provided is commensurate with employee job duties and the access needs of software accounts.*

4. Controls used to confirm the identity of CAS users were weak in several respects.

MnSCU did not deploy sufficient controls to secure accounts that have access to the CAS related systems. These controls would make it more difficult for unauthorized individuals to compromise the identity of legitimate system users. MnSCU also allowed some employees to share accounts, thereby diminishing the ability to trace certain actions to specific people. Information security relies on two fundamental principles: 1) positively confirming the identity of system users and 2) always having a mechanism to trace critical activities to specific individuals. Choosing not to vigorously enforce these principles exposes the systems and their data to unnecessary risks.

MnSCU did not configure some systems to enforce strong password controls. Strong password controls are critical because they help prevent hackers from assuming the identity of legitimate system users. Most computer operating, database management, and application systems have features that can be customized to enforce strong password controls. For example, features can be enabled that prevent users from selecting blank passwords or words that are in the dictionary. Also, features can be enabled to suspend unused accounts or accounts when the incorrect password is used too many times. We examined these and other customizable security features and found many weaknesses. In some cases, the department did not implement important security controls. It is also worthy to note that CAS was not designed to include several of these critical controls.

The department did not change one account's default password on a purchased software product. Many purchased software products come with default user accounts and passwords. It is important to immediately change default passwords because they provide an easy avenue for hackers to gain unauthorized access. In fact, lists of default accounts and passwords for most purchased software products are available on the Internet. As part of our testing, we were able to take control of this account because MnSCU failed to change the default password.

Finally, some information technology professionals share accounts with extremely powerful security clearances. Sharing passwords is always unacceptable because it destroys individual accountability. Once a password has been shared, it is virtually impossible to prove that a specific person initiated a specific computerized transaction.

Recommendations

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

- *MnSCU should work with the CAS vendor to resolve the system's security shortcomings or devise alternative controls.*

- *MnSCU should immediately change the default passwords after installing new software.*

- *MnSCU should implement controls to ensure that critical system activities can be traced to specific individuals.*

5. MnSCU did not remove unnecessary and insecure services from its CAS server or perform important system maintenance procedures in a timely manner.

We identified several services on the CAS server that were unnecessary. The term "service" refers to a computer program that runs continuously, listening for specific commands. Services are typically activated by default after installing a computer operating system and are needed to perform basic functions, such as logging in. However, many services are not necessary and could lead to security breaches if not removed. In fact, several of the unnecessary services we identified were susceptible to common hacker exploits. We also found other insecure services that were used by MnSCU to conduct business, even though secure replacements were available but not deployed.

We also identified some security-related software patches that were not installed on the systems that support CAS. MnSCU uses several commercially available software packages. Unfortunately, computer hackers routinely discover and exploit flaws in commercial software to gain unauthorized access to organizations' computer systems. When these exploits occur, reputable vendors immediately develop and publish software patches to correct their product's deficiencies. Organizations that do not promptly install these software patches make their systems easier targets for computer hackers.

Identifying and patching computers can be an extremely daunting task. To improve controls, the department needs to define, document, and stringently enforce its patch management policies and procedures.

Recommendations

- *MnSCU should remove all unnecessary services.*

- *MnSCU should replace all remaining services that have known security weaknesses with more secure programs.*

- *MnSCU should implement procedures to promptly install security-related patches.*

6. MnSCU does not adequately monitor DARS and CAS for unauthorized or inappropriate access.

MnSCU lacked important controls to detect and promptly respond to security-related events, such as unauthorized access attempts. The best security controls are those that prevent inappropriate events from happening. Unfortunately, it is virtually impossible to design flawless preventive defenses. Unscrupulous individuals constantly discover new security exploits and use that knowledge to penetrate organizations with many layers of preventive defenses. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack. Since response time is critical during an attack, every organization also must have decisive incident response procedures. Organizations that do not have effective procedures may not discover they are completely unsecured until after extensive damage has been done.

MnSCU did not adequately assess its monitoring needs or actively monitor security-related events. Some commercial software products used by MnSCU can be customized to log certain types of unusual events and alert specific individuals. However, in some cases these products were not configured to log any events. In others, employees did not routinely review the logged activities. Employees told us they did not have sufficient resources to review logs on a regular basis.

Recommendation

- *MnSCU should assess its monitoring needs and develop procedures to regularly monitor its systems.*

OFFICE OF THE CHANCELOR

500 WELLS FARGO PLACE
30 EAST SEVENTH STREET
ST. PAUL, MN 55101-4946

ph 651.296.8012
fx 651.297.5550
www.mnscu.edu

Minnesota
State Colleges
& Universities

July 6, 2004

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 selected components of the Degree Audit Report (DARS) and Course Applicability (CAS) Systems currently used by the Minnesota State Colleges and Universities. We appreciate the opportunity to work with your auditors to identify and resolve security issues and protect the data availability and integrity of our systems. In particular, the findings will help us resolve identified issues before the CAS system is moved into full production mode across the entire System.

Both DARS and CAS are purchased off the shelf commercial systems and as such were not developed with MnSCU's environment or security requirements in place. We are currently working with Miami University of Ohio to fix existing security risks in their DARS software product, as options for MnSCU ITS correcting them would be extremely difficult to implement and expensive to maintain. Over 150 colleges and universities across the country are also users of this system, and it is our intent to leverage this existing user base to correct security design issues.

We also agree that CAS security issues need to be addressed; since the application is currently used at only nine institutions, risk is currently limited. We believe we can significantly improve the security environment prior to system wide implementation later this year.

Our response to address the current audit findings follows.

Sincerely,

/s/ Ken Niemi

Ken Niemi
Vice Chancellor for Information Technology & CIO

Finding 1:

- MnSCU did not design and implement an effective security infrastructure for DARS and CAS.

Response:

- o *DARS is a COBOL program running on Rdb in the VMS environment and is a part of the same security infrastructure applicable to ISRS. CAS, however, runs in the UNIX environment with a very different security infrastructure. Nevertheless, MnSCU agrees all its UNIX based environments require detailed standards for configuring, managing and securing the environment. ITS will develop UNIX operation system hardening procedures and apply them to all UNIX environments.*

- o *ITS recognizes the importance of proper system management practices and a new position will be requested for a UNIX system manager. When the position is filled, staff will formally begin the system management responsibility for the CAS server. A plan to divide responsibility appropriately between system administration, operations, and development is being created. After the server is turned over to the UNIX system manager the separation of critical responsibilities should be satisfied. The new UNIX system manager position will be filled by the end of the fourth quarter of calendar year 2004.*

- o *While ITS agrees that periodically testing the environment for vulnerabilities is important, current staff resources limit capabilities to accomplish this. However, after the new UNIX system manager position is filled this task will be a priority.*

Finding 2: DARS allows users to view, alter, or delete data from uncontrolled environments.

Response:

- o *MnSCU is currently working with the software vendor, Miami University of Ohio, in an attempt to have access to the DARS database changed to some form of data access other than ODBC. The expense of other options makes them cost prohibitive. ITS agrees that the DARS application has design shortcomings and will work with the vendor to eliminate ODBC access.*

Finding 3: Several accounts had excessive clearance to the DARS and CAS related systems.

Response:

- *ITS and the degree audit staff will work together to review access to DARS and CAS applications for the purpose of identifying the appropriate security levels for Office of the Chancellor staff and staff at the institutions. The new UNIX system manager will review the operating system security parameters with the data base administrator and application support developer to assure all parameters are set appropriately. The effort will be completed by the second quarter of calendar year 2005.*

Finding 4:

- Controls used to confirm the identity of CAS users were weak in several respects.

Response:

- *ITS will reassess operational management of the software, as well as document process and responsibilities within operations, security, development and server support. ITS will ensure that current password management controls are fully enforced. ITS and degree audit staff will work with the CAS vendor to resolve the product's security issues or devise alternative controls to mitigate those issues.*

Finding 5:

- MnSCU did not remove unnecessary and insecure services from its CAS server or perform important system maintenances procedures in a timely manner.

Response:

- *Activities are currently underway to have an ITS system manager harden the operating system and remove all unnecessary services. This process of hardening the operating system will be completed by the end of the fourth quarter of calendar year 2004.*

- *Appropriate patches have been applied and procedures will be implemented to ensure that up to date operating system patches are maintained.*

Recommendation 6: MnSCU does not adequately monitor DARS and CAS for unauthorized or inappropriate access.

Response:

- *The ITS operations staff will work with the system managers to establish a process to review logs for unauthorized access attempts, on a daily basis. ITS is currently reviewing a long term solution that requires all* *operating system logs to be collected to a single server where a combination of reviews can take place. When implemented, log review will be semi-automated through the use scripts or a purchased product and manually reviewed by staff positions. Procedures will be developed and documented. The operations staff log review will be implemented by the end of the third quarter of 2004.*

- *Procedures will be developed and documented for integrating customer selected and procured applications into the formal ITS structure and processes.*