Minnesota State Colleges and Universities

Selected Scope Audit of the Student Information System Tuition and Accounts Receivable Module as of June 1999

October 1999

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 296-1727

Financial Audit Division
Office of the Legislative Auditor
State of Minnesota

99-53

Centennial Office Building, Saint Paul, MN 55155 ● 651/296-4708

SUMMARY

State of Minnesota
Office of the Legislative Auditor
1st Floor Centennial Building
658 Cedar Street • St. Paul, MN 55155
(651)296-1727 • FAX (651)296-4712
TDD Relay: 1-800-627-3529
email: auditor@state.mn.us
URL: http://www.auditor.leg.state.mn.us

Minnesota State Colleges and Universities
Information System Application Review

Selected Scope Audit of the Student Information System (SIS)
Tuition and Accounts Receivable Module
As of June 1999

Public Release Date: October 1, 1999 No. 99-53

Background

Minnesota State Colleges and Universities (MnSCU) began operations on July 1, 1995, and includes three state-level higher education systems: state universities, community colleges, and technical colleges. Currently, MnSCU consists of 36 different institutions at 54 campus locations with estimated tuition revenues of $245 million for fiscal year 1999.

MnSCU designed and developed its computerized business systems in-house. The accounts receivable module of the Student Information System (SIS) controls tuition assessments, collections, and outstanding receivables by automatically:

- assessing tuition as a result of registration activity;
- charging course fees, along with standard and special student fees;
- posting collections against student tuition and fee charges;
- applying financial aid funds to the students' accounts; and
- posting the appropriate accounting transactions.

Three pilot schools began using the new accounts receivable module in the fall of 1997. The remaining institutions were phased into the module.

Selected Audit Areas and Conclusions

Our audit focused on the application controls over tuition and fee assessments, collections, student accounts receivable balances, and the accounting transactions that result from these activities and processes. Application security controls were reviewed. We utilized MnSCU databases to assess the integrity of the rate tables, registration and collection data, and resulting calculations and accounting transactions.

We found that the system properly assessed tuition and fees, applied collections and financial aid properly, maintained student balances, and posted the appropriate accounting entries. We did, however, note some concerns with application security controls. Two security groups were designed with excessive clearance to incompatible functions and institutions did not adequately restrict access based on job responsibilities. We also found that negative receipt transactions were vulnerable, and management reports are needed for registration cancellations, waivers, and aging of unpaid accounts receivables.

The MnSCU system office agreed with the findings and recommendations contained in the audit report and are working to resolve the issues identified.

STATE OF MINNESOTA
OFFICE OF THE LEGISLATIVE AUDITOR
JAMES R. NOBLES, LEGISLATIVE AUDITOR

Representative Dan McElroy, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

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

Members of the Minnesota State Colleges and Universities Board of Trustees

We have performed a selected scope information systems audit as further explained in Chapter 1. We emphasize this has not been a complete audit of all aspects of MnSCU's computer systems. Our audit focused on the application controls over MnSCU's Student Information System modules impacting student tuition and fee assessments, collections, outstanding accounts receivable balances, and the resulting accounting transactions. The audit Summary highlights the specific audit objectives and our conclusions. We discuss these issues more fully in the individual chapters of this report.

We conducted our audit in accordance with *Government Auditing Standards*, as issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of management controls relevant to the audit. The standards also require that we design the audit to provide reasonable assurance that the Minnesota State Colleges and Universities complied with the provisions of laws, regulations, contracts, and grants significant to the audit. The management of MnSCU 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 Minnesota State Colleges and Universities. This restriction is not intended to limit the distribution of this report, which was released as a public document on October 1, 1999.

James R. Nobles
Legislative Auditor

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: July 8, 1999

Report Signed On: September 27, 1999

1ST FLOOR SOUTH, CENTENNIAL BUILDING ● 658 CEDAR STREET ● ST. PAUL, MN 55155
TELEPHONE 651/296-4708 ● TDD RELAY 651/297-5353 ● FAX 651/296-4712 ● WEB SITE
http://www.auditor.leg.state.mn.us

MnSCU – Student Information System Application Review

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
Keith Bispala	Senior Auditor
Jason Stauffenecker	Senior Auditor

Exit Conference

We discussed the findings and recommendations with the following representatives of the Minnesota State Colleges and Universities (MnSCU) system office on September 13, 1999:

Laura King	Vice Chancellor, Chief Financial Officer
Rosalie Greeman	Associate Vice Chancellor, Financial Reporting
Al Finlayson	Director of System Accounting
Deb Winter	Director of Campus Accounting
Dale Jarrell	System Director, Policy, Planning, and Services
John Asmussen	Executive Director, Internal Auditing
Beth Buse	Deputy Director, Internal Auditing

Chapter 1. Introduction

The Minnesota State Colleges and Universities (MnSCU) system began operations on July 1, 1995. The new MnSCU system combined two state-level higher education systems, state universities and community colleges that had previously existed as independent systems. It also incorporated several technical colleges into state government. In total, MnSCU now consists of 36 different institutions with 54 campus locations. MnSCU's colleges and universities serve approximately 230,000 students in for-credit courses, 100,000 students and 3,200 businesses through customized training, and 100,000 students in non-credit continuing education programs[1]. MnSCU estimated it would collect $245 million in tuition during fiscal year 1999[1].

Prior to the higher education merger, MnSCU made a decision to develop a collection of new computer systems, or modules, to help institutions manage their business activities. This system development effort, referred to as the Integrated Statewide Records System (ISRS), began in early 1994 and is still underway. Accounting, Human Resources (SCUPPS), and Purchasing (PCS) were among the first modules implemented. Other modules including Curriculum, Term Course, Registration, and Accounts Receivable were available for the fall 1998 semester. These four modules, and several others, have collectively been termed the Student Information System (SIS). In the fall of 1997, Moorhead State University, Metropolitan State University, and Minnesota West Community and Technical College implemented several of the modules as part of the SIS pilot. At the time of our audit, institutions continued to implement SIS on a phased-in basis.

MnSCU has been implementing its new business systems in a complex computing environment called "client server." Client server refers to a special type of environment where several different computers work together to accomplish a task. Typically, these computers are connected and communicate over a high-speed local or wide area network. With all the MnSCU modules, a user's personal computer (i.e. the client) completes a portion of the computer processing. The remaining processing occurs on a central computer at one of MnSCU's four regional data centers. Communications between campus machines and the central data center computers occur over the State of Minnesota's wide area network.

Each institution stores its business data in its own production database. MnSCU houses each institutional database at one of the four 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 users instantaneous access to their business data. In addition, an exact copy of each institution's production database is made every night. This copy, referred to as an institution's replicated database, gives users a tool for ad-hoc reporting. We used an extensive amount of data stored in institutional databases to conduct much of our audit work.

All the courses offered by an institution comprise its curriculum. The courses offered are entered in the Curriculum module and used to generate a Course Catalog. The Term Course module is

[1] Minnesota Biennial Budget, Higher Education 2000-2001.

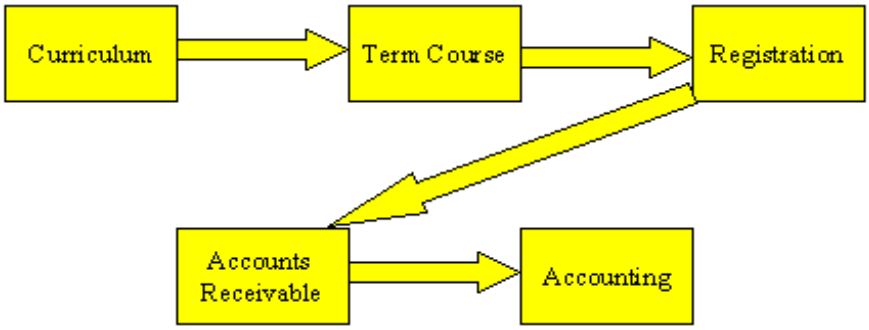
used to schedule specific courses that the institution will be offering for any given school term. Students register for particular course offerings using the Registration module. The system provides three methods of registration that include phone, web, and traditional. The traditional method requires a registration employee to obtain information from the student and then input the data into the system, while phone and web registration allow students to enter information directly into the system. The Accounts Receivable module tracks receivables from the time a student registers until their final disposition. The module automatically:

- charges tuition as a result of registration activity;
- adjusts tuition charges when courses are added or dropped;
- charges course fees, and standard and special student fees;
- posting collections against student tuition and fee charges;
- applies financial aid funds to the student's accounts; and
- posts the related accounting transactions to the appropriate accounting system cost center or general ledger.

Since the Accounts Receivable and Accounting modules are fully integrated, universities and colleges are not required to separately input or reconcile data from independent systems. The system, however, was not designed to encompass customized training assessments and collections. In addition, other receivables may be created manually. For example, student fines, rental of space, or sale of services to non-student customers are charges that an institution may create manually.

Figure 1-1 depicts the flow of information between SIS modules.

Figure 1-1
Minnesota State Colleges and Universities
Student Information System Flow of Information



MnSCU's Office of Internal Auditing performed a review of this system and released an audit report January 20, 1999, titled *Student Information System*. This report was critical of MnSCU's system development methodology, suggesting MnSCU was ill equipped to develop its own software in-house. System development occurred without the benefit of a structure that promoted user participation, testing, and acceptance. The report indicated that insufficient

resources were invested in testing the quality of software modules, developing training programs and gaining user acceptance, and documenting system design and processes.

We believe the following key concerns identified in the Internal Audit report, or through our observations, increased the risk that the system may produce erroneous information:

- SIS computerized software (application screens) were placed into production prior to being thoroughly tested. We observed several situations where campus users encountered problems with specific application screens. MnSCU dealt with these situations by alerting system users to discontinue use of the screens until they were working properly. Ideally, new and modified screens should be tested prior to release to avoid user errors and frustration.

- MnSCU lacked some technical documentation providing an understanding of system data, tables, and interrelationships. For example, there is no comprehensive data dictionary defining SIS tables and interactions. MnSCU has begun to develop user documentation describing business processes and screen information; however, technical documentation could be improved.

- MnSCU placed substantial responsibility for system design on one individual and primarily relied on that person for ongoing knowledge and understanding of the system. If this individual was to leave or transfer, MnSCU may encounter difficulties or inefficiencies in understanding key system design and logic. Ideally, the technical documentation described above would alleviate inefficiencies caused by the loss of individuals with vital system knowledge.

Because of these conditions, we felt an application review of the SIS modules would provide the MnSCU system office with assurances that data integrity and processing logic produced reasonable results.

Our audit focused on the application controls over tuition and fee assessments, collections, student accounts receivable balances, and the accounting transactions that result from each of these activities. Application controls safeguard the integrity of information gathered, stored, and processed in an organization's database. They are defined as methods of ensuring that only complete, accurate, and valid data is entered and updated in a computer system; that processing meets expectations and accomplishes the correct task; and that the integrity of data is maintained. Chapter 2 discusses the Student Information System application security controls. In Chapter 3 we reviewed system processing controls.

This page intentionally left blank.

Chapter 2. Application Security Controls

Chapter Conclusions

MnSCU did not adequately limit access privileges to its Registration and Accounts Receivable modules. Security groups were designed to promote separation of functional duties, mainly registration, collection, and accounts receivable responsibilities. However, we noted that two security groups allow excessive access to incompatible screens. We also determined that campuses did not adequately separate functional access to their Registration and Accounts Receivable modules. More specifically, MnSCU:

- ***did not provide adequate documentation for its institutions to make informed security decisions;***
- ***did not adequately monitor system access, resulting in an excessive number of users given access rights to incompatible functions; and***
- ***allowed a number of users access to multiple institutions, although their jobs may not require such access.***

MnSCU employees typically use electronic forms or computer screens to enter, modify, and delete data. MnSCU designed security groups for each of its new business systems. Each security group gives users access to a pre-defined set of computer screens. Structured security groups are critical because they provide the necessary foundation to separate incompatible business functions. Security groups can be used to limit each user to the specific computer resources and data that they need to fulfill their job responsibilities.

MnSCU developed its own security application, called the 'Menu System,' which controls access to screens. Menu System security operates in conjunction with the operating system security, which provides the initial validation of the user at the point of login. The Menu System is basically a set of relational database tables that:

- identify all users, security groups, and screens;
- link users to security groups; and
- link security groups to screens.

MnSCU designed standard system access request forms for each module. Each form contains a list of the security groups and, typically, each screen number and name that the group can access. After selecting the appropriate security groups, specified campus managers must approve the access request. Data center security administrators then enter the appropriate security transaction based on the approved request.

MnSCU – Student Information System (SIS) Application Review

Our audit focused on security groups, screens assigned to security groups, and the users assigned to security groups. As previously mentioned, however, there are additional levels of security. For example, MnSCU's operating system, Open VMS, has its own internal security module. Each user must have an Open VMS user account. Users, typically information systems staff, may also have special Open VMS privileges or other high level security access permitting them to update database tables directly by-passing the intended modules and forms. This is commonly referred to as "backdoor access." This audit did not review Open VMS or SQL security. However, during fiscal year 1997, we conducted an Information Security Review that raised concerns with these additional aspects of security. In March 1998, the MnSCU Office of Internal Auditing conducted a follow-up and issued a report indicating MnSCU had made significant progress in limiting access to critical business data. They noted, however, its information systems continue to show some vulnerability to security breaches. It is important to note that our current audit did not follow-up on these prior security concerns.

Audit Objectives and Methodology

Our review of Student Information System (SIS) menu security focused on the following objectives:

- Did MnSCU design Menu System security groups to establish an environment where incompatible duties are separated? Were compatible production screens assigned to logical security groups?
- Have campuses separated functional access by not assigning staff to incompatible security profiles?
- Are campuses adequately restricting access to a reasonable number of users, especially for tuition and fee rates and sensitive transactions?

To address these objectives, we studied the various security groups and screens designed by MnSCU, discussed security privileges with MnSCU technical and campus staff, and reviewed the types of transactions that could be performed by different security groups. Finally, using each institution's replicated database, we gathered and analyzed electronic security groups and screens assigned to campus staff.

Conclusions

MnSCU did not adequately limit access privileges to its Registration and Accounts Receivable modules. We found that two security groups did allow excessive access to incompatible screens. Also, even though MnSCU designed most security groups to promote separation of functional duties, campuses did not adequately separate access to their registration, collection, and accounts receivable functions. We think MnSCU did not provide adequate guidance for its institutions to make informed security decisions. It also did not strictly enforce separation of duties or have a mechanism to monitor incompatible access, resulting in an excessive number of users given access rights to incompatible functions. Finally, a number of users were allowed access to multiple institutions, although their jobs may not require such access.

1. Two security groups provide access to incompatible functions.

MnSCU designed two security groups that provide excessive access to incompatible screens. An accounts receivable security group was given full access to cashiering and accounts receivable functions. Users assigned to this group have the ability to receipt moneys, correct or adjust receipt transactions, waive or defer any student charges, change student residency codes, and create, adjust, or waive non-student accounts receivable balances. In addition, these users could change tuition and fee rates as well as the cost center or general ledgers that these receipts post to. Ideally, handling of receipts should be separated from the ability to assess, waive, or record charges. We found 143 users system-wide who had this full-access accounts receivable security group. Also, a previously established accounting security group was assigned similar access as described above. We found 280 users system-wide who were given this group's privileges.

Recommendation

- *MnSCU should review and modify two key security groups that allow excessive access to incompatible functions.*

2. MnSCU campuses did not adequately restrict access to their registration and accounts receivable business systems.

Security groups were designed to separate duties. However, MnSCU campuses assigned employees access to incompatible security groups. We identified the following concerns regarding campus access:

- MnSCU did not adequately document the access provided by each security group and did not have any access standards for particular job positions. We found no documentation identifying incompatible security groups to assist campus security administrators when granting access requests. Furthermore, MnSCU did not identify effective control methods to mitigate risks if an institution could not feasibly separate duties. Without this guidance, employees who complete and approve system access requests have difficulty making informed decisions. These risks are compounded for MnSCU, which has an evolving computer environment. Employees who request or approve access to these new systems may only have a limited understanding of a system's capabilities.

- MnSCU did not adequately monitor system access. As shown in Table 2-1, we found that an excessive number of users were granted access to security groups that allowed them to update critical information such as tuition rates, tuition waivers and deferments, and the residency code used to calculate a student's tuition charges. We question whether all these users have job responsibilities requiring this access.

Table 2-1
MnSCU Student Information System
Number of Users

Ability to Update:	Users
Tuition/Fee Rates	685
Registration	702
Collections	447
Waivers	415
Deferrals	453
Student Residency Code	436

Source: Auditor prepared from MnSCU Menu System Security Data.

- An excessive number of users were assigned incompatible security groups. We think that cashiers should be restricted from posting sensitive transactions that allow manipulation of recorded balances. Over 340 users assigned cashiering security privileges also had the capability to alter registration information, waive or defer registration charges, adjust or waive non-student accounts receivable balances, and change student residency codes used in the tuition calculation.

- We noted that a number of users had excessive access to multiple institutions. We found 35 users who could update the rate tables from 2 to 36 MnSCU institutions. Similarly, 32 users could process waiver or deferment transactions, or initiate changes to student residency codes used to calculate tuition and fee charges. Most of these users were MnSCU system office employees in the Finance Unit as well as the Information Technologies Service Unit. These employees may not require access to multiple colleges or universities to perform their job responsibilities.

Recommendations

- *MnSCU should adequately document access provided by each security group, develop baseline security standards for job descriptions, document potentially incompatible security groups, and identify effective methods to mitigate risks when an institution cannot separate duties.*

- *MnSCU should develop procedures to monitor system access and investigate excessive, as well as incompatible, clearances that currently exist. System access privileges should be based on job responsibilities.*

Chapter 3. System Processing

Chapter Conclusions

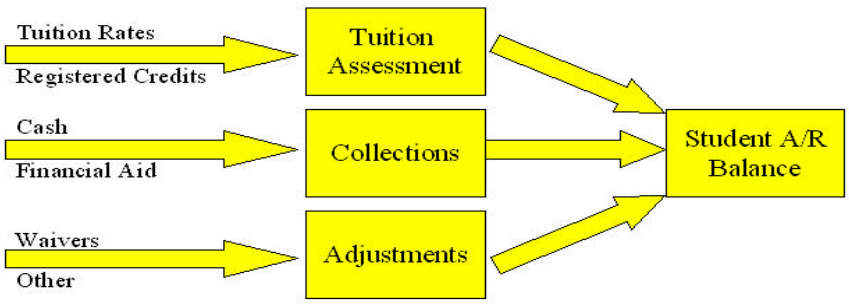
MnSCU designed a computerized accounts receivable application that integrates with other Integrated Student Records System (ISRS) modules, primarily accounting. Integrating the various registration, accounts receivable, and accounting processes minimizes the risk of human input error and avoids the need for duplicate entry or reconciling of independent subsystems. Using the system databases, for the items tested, we found that the system properly:

- ***assessed tuition and fees based on registered credits;***
- ***applied collections and financial aid funds to student accounts;***
- ***maintained student accounts receivable balances; and***
- ***posted the appropriate accounting entries.***

However, we found that MnSCU has not developed some key management control reports to address specific risks involved with certain sensitive transactions. Also, negative receipt transactions create an unnecessary risk and provide a poor audit trail.

The MnSCU Student Information System (SIS) interfaces registrations and collections to calculate individual student accounts receivable balances. Figure 3-1 shows the processing components included in the accounts receivable calculation.

Figure 3-1
Minnesota State Colleges and Universities
Student Accounts Receivable Processes



A critical result of these processes is that the system also initiates the automated posting of cash, tuition revenue, and accounts receivable balances into the MnSCU accounting system.

Tuition and Fee Assessments

Tuition and fees are assessed and billed to students automatically by the MnSCU Accounts Receivable module. Each night the system recalculates student tuition/fee charges for new registration activity. If a student registered for a course, the system checks the course record to determine the instructional unit that the course is tied to. An instructional unit, set up in the Curriculum module, is the link between the Course and the Accounts Receivable module. Next, the system checks the system tables to determine which tuition group is tied to the particular instructional unit. A tuition group allows the institution to take a number of instructional units, which will be billed in the same manner, and combine them into a group. Once the system has determined the instructional unit and tuition group, it checks the student record to determine the student's state of residency. The system then checks the course record in Term Course to determine if it is a graduate or undergraduate course. Next, the system checks the system tables to determine which rate has been entered for the applicable tuition group, residency status, and course level. Once the system has determine the appropriate rate, it checks the course record to determine the number of credits that the course is worth and multiplies tuition rate by the number of credits to calculate the student's tuition bill. As a result of the tuition calculation, the system also initiates posting of the appropriate tuition revenue accounting transactions.

Any one of three events could initiate the system tuition calculation. First, as discussed above, new registration activity triggers a nightly batch process calculation. For this type of calculation to occur, the student would have added or dropped a course in registration. Second, a cashier can perform an immediate system calculation if a student pays tuition the same day as registering. The cashier can prompt the system to recalculate that student's bill only. Finally, the campus can request a special recalculation of all students. For example, if a college needs to recalculate all students, due to late entry of course fees or a late change in tuition rates, they can request this process from their regional computer center.

Tuition and Fee Collections

Tuition and fee receipts generally come from either the student paying directly or student financial aid. When a student pays directly, a cashier would collect the money and post the receipt to the student's account. The system applies the receipt to the student's tuition and fee charges in order of priority, which is pre-determined by each institution, and then posts the appropriate accounting transactions. On a daily basis, cashiers should close out their cash drawer and another individual should compare collections to receipts recorded in the system.

Funds applied is the process by which financial aid funds are posted against each student's outstanding tuition and fee charges. This process occurs in the evening in a batch process. Each institution determines the frequency of the batch process. In all cases, financial aid funds applied to student accounts are run after the tuition re-calculation process to ensure that new activity is included. Each institution sets the order in which each type of financial aid is applied and the order in which specific charges are offset by financial aid. Certain sources of financial aid may have restrictions on their use requiring each institution to designate the charges that cannot be paid for by each type of aid. For example, financial aid funds cannot be applied against outstanding parking or library fines. Throughout the funds applied process, the system posts the appropriate accounting entries impacting the tuition revenue and financial aid accounts.

The funds applied process relies on financial aid award data stored in each institution's database. Depending on the institution, this data may come from different sources. MnSCU has developed its own, fully integrated, Financial Aid module. For universities and colleges using this module, awards are automatically stored in the institution's database. MnSCU, however, has not required its institutions to implement the module. The majority of institutions are using one of two other PC-based systems: SAFE and SARA. MnSCU has written computer programs that upload, or interface, detailed data from SARA and SAFE and post it to the financial aid awards table.

Students Accounts Receivable Balances and Reporting

As a result of the activity described above, and other processes, the system calculates an accounts receivable balance for each student. MnSCU has developed some pre-defined reports to help institutions identify and manage their unpaid accounts receivable balances. We also noted that institutions have begun using their replicated databases for ad-hoc reporting purposes.

Audit Objectives and Methodology

The primary objectives of our review were to determine the adequacy of application processing and controls ensuring the integrity of:

- tuition and fee assessments;
- tuition and fee collections, including student financial aid funds applied;
- student accounts receivable balances; and
- accounting transactions.

To address this objective we interviewed MnSCU staff from the system office and pilot institutions, reviewed user documentation, and studied the related tables in the MnSCU databases to gain an understanding of system controls and processing. We primarily utilized a database query tool and the data stored in MnSCU's replicated databases to determine whether logical calculations were derived, student account balances are properly impacted, and the system accurately posted the appropriate accounting transactions.

Conclusions

MnSCU designed a computerized accounts receivable application that integrates with other Integrated Student Records System (ISRS) modules, primarily accounting. Integrating the various registration, accounts receivable, and accounting processes minimizes the risk of human input error and avoids the need for duplicate entry or reconciling of independent subsystems. Using the system databases, for the items tested, we found that the system properly:

- assessed tuition and fees based on registered credits;
- applied collections and financial aid funds to student accounts;
- maintained student accounts receivable balances; and
- posted the appropriate accounting entries.

However, we found that MnSCU has not developed some key management control reports to address specific risks involved with certain sensitive transactions. Control reports would also assist management in making informed business decisions. Also, negative receipt transactions create an unnecessary risk and provide a poor audit trail.

3. MnSCU has not developed key management reports to help institutions address specific risks and aid management in making informed decisions.

MnSCU did not develop key reports to alert management to certain high-risk transactions and to facilitate informed management decisions. Either standard production database reports or replicated database queries are needed to effectively monitor or control certain financial activities. Currently, standard reports that access the production databases do not identify these transactions. Campuses can use replicated database queries to produce this information, but this process may create additional risk and difficulty. Compiling information from replicated databases requires users to have significant knowledge of relational databases, database structures, and database query tools. It also increases the risk of inaccurate reports since users can inappropriately screen or filter data. In addition, a key system flaw allows users with update capabilities in the production database to also alter data in the replicated database producing inaccurate results. We noted three key reports that would aid management in controlling tuition revenue processing:

- The computerized accounts receivable application allows users to eliminate a student's tuition and fee charges by backdating registration cancellation records. MnSCU Policy 5.8 *Refunds, Withdrawals, and Waivers* allow institutions discretion when canceling tuition charges. For example, a student is allowed to drop a class, without obligation, if done prior to the institution's established "drop date." At any time, system users can backdate a student's drop date to reflect a date prior to the required drop date. These transactions are particularly sensitive since they eliminate the student's obligation and reduce the amount earned by the institution. These transactions should be documented and specifically authorized by management. MnSCU has not developed system reports to alert management about the volume of these transactions.

- MnSCU has not developed waiver reports to help management monitor the validity and extent of such transactions. We noted waivers totaling $4.4 million were posted during fiscal year 1999. Waiver transactions are highly sensitive since they reduce or eliminate a student or non-student charge and the amount due to the college. Examples include employee waivers provided as a benefit in their bargaining agreement, student waivers for medical reasons or significant personal reasons, or where a balance needs to be adjusted as the result of an error. A report identifying waivers is critical because an excessive number of users have the ability to produce these system transactions.

- MnSCU has not developed a standard accounts receivable aging report or write-off report. Aging reports provide a valuable tool for management decisions on policies for collecting delinquent accounts, as well as writing off old uncollectible balances. Write-offs are particularly sensitive since they reduce the amount due to the institution. Similar to other transactions that reduce the amount collected, write-offs need to be documented and authorized.

Recommendation

- *MnSCU should develop key reports for cancelled registrations, waivers, and uncollectible or written-off balances to help management make informed decisions and mitigate the risk of unauthorized transactions occurring and going undetected.*

4. Negative receipt transactions provide a poor audit trail and create an unnecessary risk exposure.

We noted a key risk resulted from the use of negative receipt transactions. These transactions create a significant vulnerability since users that handle cash could potentially conceal theft. Negative receipt transactions provide cashiers with the ability to manipulate the accounting system to agree with the cash deposited. Any transaction that reduces the cash and revenue collected should be documented and properly authorized by someone independent of the collection process, typically a supervisor.

At the time of our audit, campus users could initiate a negative transaction using the receipts screen normally used to process collections. For example, if a cashier recorded a $100 receipt, but wanted to reduce it to $50, the accounting system would simply record a $50 decrease in cash and revenue, providing a poor audit trail. Alternatively, if the system correction screen was used, the accounting system would reverse the original transaction totaling $100 and also record the correct transaction totaling $50, providing a sufficient audit trail.

MnSCU has recognized the high-risk nature of performing a negative transaction using a receipt screen and has since removed that capability from two of the three security groups that previously had it. We found that approximately 200 users had the remaining security group that still allows this type of transaction. While removing the capability from two groups was an improvement, we question the need to allow any user the ability of entering negative receipts on a receipt screen rather than using the receipt correction screen.

Recommendation

- *System users should be required to use the appropriate correction screens to perform any reductions to receipt transactions.*

This page intentionally left blank.

MnSCU

Minnesota State Colleges & Universities

September 24, 1999

Mr. James 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 Minnesota State Colleges and Universities Information Systems Application Review of the accounts receivable module of the Integrated Student Information System (ISRS). Development and implementation of the student information system (SIS) was an ambitious undertaking. The system is necessary to provide a single integrated system that accurately and consistently determines tuition and fee amounts for each student, applies collections and financial aid, and maintains student accounts and posts accounting entries.

Please extend our thanks to Brad White, audit manager and Eric Wion, auditor-in-charge for their efforts in this systems review. We are pleased that you found that the system accomplished these functions properly. While we feel we have been successful in this endeavor we recognize the need for improvement. With the last two institutions completing conversion in July we can devote more resources to remedying problems, including those in your report.

We have already made significant improvements in our systems development efforts since the first institutions implemented ISRS. We now have a quality assurance unit in place to test all systems changes before they are placed in production. We have increased documentation of the business processes supported by these systems. We have significantly extended the availability of detail system data through the use of replicated databases. We have a very active user community that provides input to systems decisions and helps set priorities for improvements. Our efforts are devoted to continually improving all of the systems supporting MnSCU students and all of our institutions.

Our plans to address the audit findings are attached.

Warmest Regards,

Laura M. King
Vice Chancellor
Chief Financial Officer

Enc.

500 World Trade Center 30 East Seventh Street St. Paul, Minnesota 55101
651.296.8012 Facsimile 651.297.5550 TDD 651.282.2660

MnSCU Information System Application Review
Response to findings

September 24, 1999

Recommendation 1 : MnSCU should review and modify two key security groups that allow excessive access to incompatible functions.

Response: Over the next month, after identifying all of those users assigned to these two security groups we will notify them that the groups will be significantly altered to eliminate the incompatible accesses. We will provide information on the access provided by related security groups. We will also instruct effected institutions to review the access needs of the users involved and determine the appropriate security group necessary to accomplish the user's assigned duties.

We need to proceed with care to ensure that our actions don't result in users being unable to perform their job duties because they no longer have the necessary access. Thus, we cannot make the changes to the security groups until necessary alternate security groups have been identified and activated for each effected user. We expect to complete this process for the accounts receivable security group by the end of October and for the second group by the end of November. Ken Niemi, Chief Information Officer and Rosalie Greeman, Associate Vice Chancellor for Financial Reporting will ensure completion of this plan.

Recommendation 2:

- MnSCU should adequately document access provided by each security group, develop baseline security standards for job descriptions, document potentially incompatible security groups, and identify effective methods to mitigate risks when an institution cannot separate duties.

- MnSCU should develop procedures to monitor system access and investigate excessive, as well as incompatible, clearances that currently exist. System access privileges should be based on job responsibilities.

Response: We will provide documentation on the access rights provided by each security group and suggest the appropriate group for typical job responsibilities. Where it is not possible for an institution to avoid assigning incompatible security rights we will identify possible alternatives to mitigate the resulting security risks.

As a part of this effort we will create a report that will identify on an exception basis instances where incompatible security groups have been assigned to one individual. When instances of incompatible access rights have been assigned we will request that the institution provide the system office with an adequate plan for mitigating the risks incurred because of the incompatible rights assigned. All affected areas, finance, human resources, student affairs and information services will share in the responsibility for this effort. Expected completion date is January 31.

Recommendation 3: MnSCU should develop key reports for cancelled registrations, waivers and uncollectible or written-off balances to help management make informed decisions and mitigate the risk of unauthorized transactions occurring and going undetected.

Response: Use of the warehouse and replicated databases is a major component of our reporting strategy. This supports the Board of Trustees goal of maximum flexibility for each institution to manage their individual programs. It also is the best solution given the demand on the limited resources of the information technology services division.

We will work with the institutions to identify the reports needed to manage these events. Reports will be developed, either standard reports and/or queries for the replicated databases. We expect that in some cases a standard report will be sufficient but some institutions may want to see all instances of cancelled registrations, waivers and write-offs of accounts and while others will want to see only exceptions or statistics and trends to determine if there is a problem.

Our goal will be to be sure that each institution has some means to monitor these activities. If a standard report will not meet the needs of institutions we will provide assistance to ensure that the queries are used

properly. Financial reporting and information services share responsibility for completion of this effort. We expect to have standard queries ready by November 15. If a standard report is identified as the best solution, the completion date will be dependent on other systems priorities. Responsible persons are Ken Niemi, Chief Information Officer and Rosalie Greeman, Associate Vice Chancellor for Financial Reporting.

Recommendation 4: System users should be required to use the appropriate correction screens to perform any reductions to receipt transactions.

Response: We will deactivate the negative receipt transaction unless we determine there is a legitimate need, in limited circumstances, for such a transaction. Until this can be accomplished we will develop a report, standard or query based, to report all instances of such transactions for each institution's review. Query for listing all negative receipt transactions will be available by October 31and the decision to deactivate, or not will be made by the end of November after getting input from users. Ken Niemi, Chief Information Officer and Rosalie Greeman, Associate Vice Chancellor for Financial Reporting are responsible for ensuring completion.