OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Minnesota State Colleges and Universities
Data Warehouse Controls
Information Technology Audit

JULY 15, 2004 **04-29**

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 data warehouse currently used by the Minnesota State Colleges and Universities (MnSCU). Our audit scope was limited to the security controls and the data extract and load process. The Report Summary highlights our overall audit conclusions. The specific audit objectives and conclusions are contained in the individual chapters of this report.

We selected the MnSCU data warehouse for audit based on its increasing value and role in MnSCU's management decision making. In addition, the data warehouse has become the primary audit resource used by our office in conducting MnSCU campus audits.

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 in the data warehouse.

To meet the audit objectives, we interviewed the information technology professionals at MnSCU who managed the warehouse and designed its data integrity controls. We also analyzed security data from the operating system and database management system underlying the MnSCU data warehouse. Finally, we analyzed network security controls using specialized vulnerability assessment software.

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: April 16, 2004
Report Signed On: July 12, 2004

Minnesota State Colleges and Universities
Data Warehouse Controls

Table of Contents

Audit Participation

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

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Brad White, CPA, CISA	Audit Manager
Neal Dawson, CPA, CISA	Auditor-in-Charge
Eric Wion, CPA, CISA	Information Technology Auditor
Sally Tefera	Intern

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
Joanne Chabot	Deputy Chief Information Officer
Bev Shuft	Security Director
Gerry Rushenberg	System Director – Management Information
John Asmussen	Executive Director – Internal Auditing
Beth Buse	Deputy Director – Internal Auditing

Minnesota State Colleges and Universities
Data Warehouse Controls
Information Technology Audit

Report Summary

Key Conclusion:

The Minnesota State Colleges and Universities (MnSCU) developed procedures to extract and load data from source computer systems into its data warehouse. However, we identified some concerns with the security infrastructure and standards for the design and testing of data transferred into the warehouse.

Findings:

- MnSCU has not documented existing procedures and has not formalized procedures to ensure that data transferred from its source business systems to the data warehouse is accurate and complete. (Finding 1, page 7)
- MnSCU needs to improve its security over the operating system and database underlying the data warehouse. (Finding 2, page 9)
- One employee performs incompatible duties. (Finding 3, page 10)

The audit report contained 3 audit findings relating to internal controls over MnSCU's data warehouse.

Audit Scope:

Audit Period:
As of April 2004

Selected Audit Areas:
- Security
- Data Extract and Load

Agency Background:

MnSCU's data warehouse is a management information tool and not a transactional accounting system. The warehouse is used to provide data to support a wide array of critical business decisions that are made at all levels of the organization. MnSCU houses individual campus databases at one of four regional data centers. The data warehouse allows MnSCU to produce system-wide reports from these decentralized databases.

This page intentionally left blank

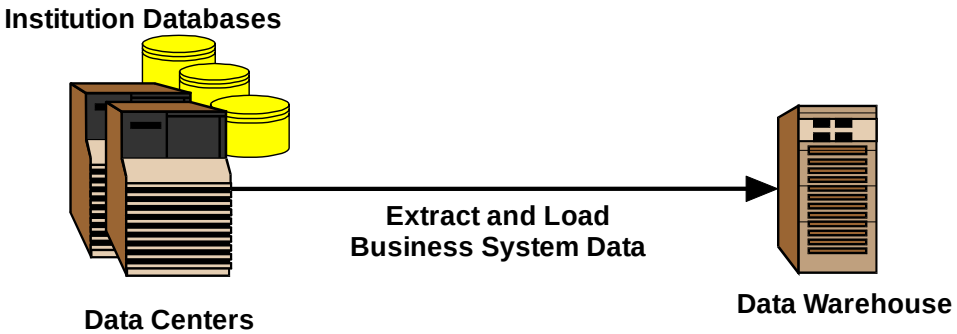
Chapter 1. Introduction

This audit analyzed how the Minnesota State Colleges and Universities (MnSCU) control the accuracy and completeness of information in its data warehouse. The data housed in MnSCU's warehouse is used to support a wide array of critical business decisions that are made by many people at all levels of the organization, including the Board of Trustees, the Chancellor and his executive team, campus presidents, and the many business departments at each campus. Business users of a data warehouse expect it to be a reliable place for them to access complete, accurate, and trustworthy business information. Every encounter with bad data in a warehouse erodes the trust and diminishes acceptance of the data warehouse.

MnSCU developed a central data warehouse because it was extremely difficult to produce system-wide reports from existing decentralized databases. MnSCU's computer system, referred to as the Integrated Statewide Records System (ISRS), consists of over 20 modules, including accounting, human resources, purchasing, student registration, accounts receivable, and financial aid. Although MnSCU campuses all use the same system, each institution stores its business data in its own production database. MnSCU houses the institutional databases at one of four regional data centers and connects them to the central computer at that site. Also, an exact copy of each institution's database is made. These copies, called replicated databases, have been the primary tool for adhoc reporting in the past. In October 1999, the Board of Trustees asked that several management reports be developed to track system-wide activity. Achieving this reporting requirement was difficult in MnSCU's decentralized computer environment. As a result, MnSCU began development of the data warehouse.

MnSCU's data warehouse has quickly become a significant tool to help support many needs. The data warehouse started out from a small Microsoft Access database of about 20 tables to support the initial request of the board. Today, the warehouse has grown to a large-scale enterprise database and supports key management reports. As depicted in Figure 1, the warehouse pulls data from each of the MnSCU institutional databases. Extract programs run nightly to update key data so that end users have up-to-date data. At the time of our review, the data warehouse contained over 300 tables with over 200 million rows of data, and it had over 400 active users.

Figure 1
MnSCU Data Warehouse Environment



Source: Auditor prepared.

MnSCU has a small team of five staff who are responsible for virtually all aspects of managing the warehouse. Managing the data warehouse is a challenge for such a small team, and we believe it will become increasingly difficult in the future. The following factors may impact the future success of the data warehouse.

- The team is continually confronted with adhoc requests for special data and reports. The time and resources necessary to respond to these requests is high.

- In addition to managing the data warehouse itself, the team is also responsible for supporting the tools used by business users to query the data in the warehouse. This includes supporting specialized software and writing all of the standard queries or reports that are needed.

- Although campus staff utilize the warehouse more and more, each campus is still highly dependent on its "replicated database" (an exact copy of its ISRS database) for data. Campuses have spent significant time and resources building queries or reports to meet their business needs. MnSCU's goal is to ultimately eliminate each institution's replicated database and have their data needs met via the warehouse. When this occurs, the demand placed on the warehouse team could be significant.

Our data integrity audit included a review of the procedures and tools used to protect information warehouse data from unauthorized changes. We also analyzed controls over loading information warehouse data tables. Finally, we analyzed how the department synchronizes data maintenance between ISRS and the data warehouse. Chapter 2 discusses the scope of our work and the conclusions that we reached.

Chapter 2. Warehouse Data Integrity Controls

Chapter Conclusions

MnSCU developed some control procedures to ensure that the data extracted from the source systems is complete and accurately loaded into the data warehouse. However, MnSCU did not document existing procedures and does not have formal standards to control the design, testing, and implementation of the data extract and load processes.

The security infrastructure for data warehouse needs improvement. MnSCU established strong security over end users; however, security controls for its key information technology (IT) professionals and related system needs improvement. MnSCU does not have a formal security plan for its warehouse environment, including policies, procedures, and standards needed to guide security. In addition, one key MnSCU IT professional performs many critical, incompatible duties. These duties should be integrated into the existing operating and security functions.

Audit Objectives

We designed our data integrity work on the warehouse to address the following questions:

- Does MnSCU have controlled procedures to ensure that data transferred from source business systems to the warehouse is accurate and complete?

- Does MnSCU have an appropriate security infrastructure to prevent unauthorized changes to warehouse data?

Background

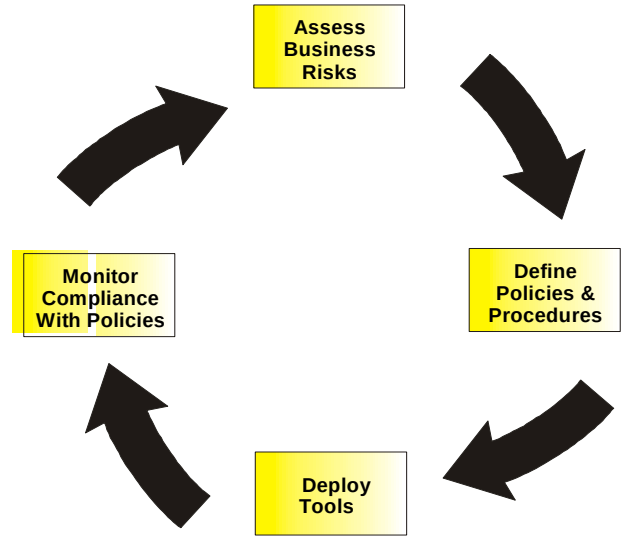
MnSCU created a valuable data warehouse to provide management with system-wide analysis of its decentralized data maintained by individual universities and colleges. Data integrity controls are critical to ensure the accuracy and completeness of warehouse data. In a data warehouse, data integrity controls encompass three major control elements:

- *security,*
- *extract and load programs, and*
- *synchronization of data maintenance.*

We discuss these three elements in more detail as follows:

- *Strong security controls need to be in place to prevent unauthorized changes to the warehouse data.*

Figure 2-1
Security Management Lifecycle



Source: Auditor prepared.

Security controls include information security over the database management system, host operating systems, and any related systems that may affect integrity of the warehouse data. Such systems may include systems that house extract source code or systems that run the extract and load processes. These systems need to be tightly secured.

One method to ensure good security is the adoption of formal security policies, standards, and procedures for a data warehouse system. As illustrated in Figure 2-1, organizations typically begin this process by performing a detailed risk analysis to identify potential vulnerabilities. The results of this analysis help organizations design policies and procedures to reduce their security exposures to a level that management is willing to accept. Security professionals then deploy tools, such as access control software, to enforce the policies and procedures that management sanctioned. Information provided by these tools helps organizations monitor compliance with their policies and procedures and fine-tune subsequent risk assessments in the ongoing security management lifecycle. These fundamental activities allow an organization to proactively manage information security risks, rather than react to problems after they have occurred.

- *Strong controls need to exist over the processes used to extract data from the source system and load the data into the warehouse.*

Data integrity controls need to begin with the design and development of the data extract and load programs. These programs need to follow stringent standards and procedures in the design, development, testing, and migration stages.

In addition, critical controls also need to exist during the ongoing execution stages of the extract and load programs. Mechanisms need to be in place to ensure that the extracted data loaded into the warehouse is accurate and complete. Checksums and record counts are common items quantified to ensure data integrity. Specialized third-party software for extract and load procedures often have similar built-in controls.

- *Strong controls need to be in place to ensure that any data maintenance on the source systems is synchronized with the warehouse.*

There may be instances where historical data or data structures in the source business system changes. It is important that these changes also be recorded in the data warehouse. Typical controls include formal procedures to involve warehouse IT professionals in any proposed data maintenance changes to production systems and databases. In addition, the extract programs may have built-in controls to detect any changes in historical data.

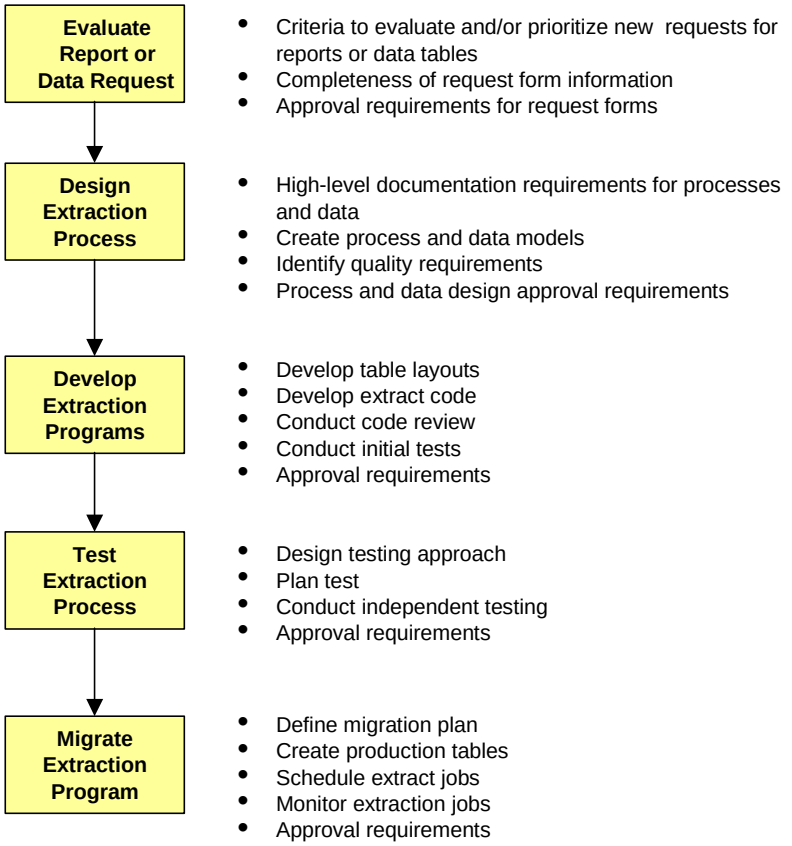
Findings and Recommendations

1. MnSCU has not documented existing procedures and has not developed formal standards and procedures for designing, testing, and migrating the processes used to extract data from its source business systems.

Currently, there is very little formality surrounding the program design, testing, and implementation of the data extract and load programs. Several individuals were involved in the development of the load and extract programs. We saw little evidence that a standard development lifecycle was followed.

Implementation of an extract process development life cycle not only ensures consistency, but it also helps minimize system development risks. Figure 2-2 defines a common development lifecycle.

Figure 2-2
Extract Process Development Life Cycle



Source: Auditor prepared.

In addition to strong development standards, MnSCU production system change control procedures should include the warehouse systems. We saw informal notification of warehouse staff when system changes or data maintenance occurred on the production source systems. The MnSCU data warehouse team often became aware of changes to production via a quality control email list serve. As a result, there was little opportunity for the warehouse staff to be actively involved in production changes that ultimately impacted the warehouse data environment.

Recommendation

- *MnSCU should develop standards and procedures for developing, testing, and implementing the extract and load programs. In addition, production change control standards and procedures should be extended to the warehouse system.*

2. MnSCU has not developed security policies, procedures, and standards for the data warehouse.

MnSCU had many security shortcomings relating to access granted to IT professionals and the security configurations for the warehouse-related systems. We found the following weaknesses:

- **Data management team employees had excessive access to warehouse-related systems.** These employees were granted special database management privileges that allow very powerful access. These privileges are typically reserved for database administrators and system level accounts. In addition, administrator access was granted to these employees on the file servers used to run the extract and load program and on the warehouse-related web servers. Administrator access should only be granted to system administrators.

- **Some end users could indirectly gain unauthorized access on the database.** We found a scenario where highly knowledgeable end users could potentially gain access through an obscure security setting. With the proper software, the user could gain broad and excessive access to the database. This particular security setting is discouraged because of its inherent high-risk security implications.

- **Several unnecessary network services and software were installed and actively running on the MnSCU warehouse production servers**. Many of these services were installed by default. Default services, such as telnet, ftp, and unused web servers, are commonly susceptible to many known vulnerabilities and pose additional risks to the servers.

  In addition, we found one instance where new web application software was installed on a web server for the warehouse. MnSCU was testing this application server and did not take the application off-line when it finished the testing. Typically, default test installations are almost always susceptible to security risks. In fact, this software was vulnerable to a known security vulnerability because the system was not properly configured. New software used for test purposes should only be installed in a controlled test environment. In addition, all software on production machines should be installed and configured by an authorized system administrator. System administrators are in a better position to properly configure software and to keep abreast on current security vulnerabilities.

  Fortunately, the security risks of many of these services (except the web server) are reduced because MnSCU does have firewalls that block access to these servers. However, reliance should not be placed solely on the firewall controls and steps should be taken to ensure that only required services are running on production systems.

- **MnSCU did not have sufficient controls to ensure that critical software was updated or patched in a timely manner.** Computer hackers routinely discover and exploit flaws in commercial software to gain unauthorized access to an organization's computer systems. When these exploits occur, reputable vendors immediately develop and publish software patches to correct the deficiencies in their products. Organizations that do not promptly install these software patches make their systems easy targets for computer hackers. We identified some software patches that were not installed on the computers that supported MnSCU data warehouse systems. Although these computers reside behind the firewall and would protect the server from many of the known security exploits, steps should be taken to keep the systems up-to-date with the latest recommended security patches on a regular and consistent basis.

Of greatest concern, MnSCU has not conducted formal information technology risk assessments or documented baseline security procedures and standards for its data warehouse environment. These security program shortcomings contributed to a wide array of security weaknesses that we brought to management's attention. Left unaddressed, these shortcomings could lead to a further degradation of security controls.

As illustrated in Figure 2-1, these and other important security decisions are the product of an ongoing risk management process. Most risk management methodologies include steps to identify potential vulnerabilities, estimate the likelihood of their exploit, and assess the potential impact. The resulting risk assessment data helps organizations design security policies, procedures, and detailed standards that are commensurate with risk.

Though management communicated its commitment to security in broad policies, it did not transform these policies into detailed security standards for the warehouse systems. 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.

Recommendations

- *MnSCU should perform periodic information technology risk assessments and use that information to develop detailed security baselines for its systems.*

- *MnSCU should periodically validate the adequacy of its controls through independent assessments.*

3. One MnSCU employee performs many duties that are often considered incompatible.

One individual is virtually responsible for almost all of the technological aspects of the MnSCU data warehouse. The employee:

- has access to the program extract and load code,
- schedules and monitors extract and load jobs,
- re-runs failed extract and load jobs,
- administers key software used for extract and load process,
- administers related web server software,
- performs database administrator functions, such as creating and maintaining tables and indexes, and
- performs database security over tables and users, including the maintenance of key warehouse audit logs.

To further compound this issue, all extract and load programs run under this individual's personal accounts. Security requirements often differ between a program and an individual's personal accounts.

Ideally, many of the warehouse functions should be separated so that there is a balance between the development, testing, migration, and operation of the warehouse environment. There should be a separation between access to program source code and actual code used in production. These controls are commonly called 'change control.' Change control ensures that production code has been adequately tested and properly secured. Developers should not have access to production code. In addition, separation also needs to exist in the daily operations of the load and extract programs. Separate individuals should be responsible for scheduling and monitoring programs. Finally, designated system or database administrators should perform administrative functions, such as software configuration or database table maintenance.

The MnSCU data warehouse team is small, comprised of five individuals. Separating duties within the data management team may be a difficult challenge. MnSCU should explore other options to separate duties, involving existing operating and security functions, or develop mitigating controls. MnSCU may be able to use other staff resources for change control, including personnel involved with operations and system administration. Common mitigating controls may include:

- Separate, noninteractive system accounts should be used to run programs and own data tables.

- Independent and periodic review of the integrity of the program code used to extract and load data. For example, integrity check sums can be performed on a program code and compared to a baseline on a periodic basis.

- Independent review of program logs, error logs, and database audit logs. Access to logs needs to be secured to prevent unauthorized changes.

- System and database access controls should be limited to the least amount of access needed.

Recommendation

- *MnSCU should explore options to either separate the duties of critical warehouse functions or develop strong mitigating controls.*

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 the Minnesota State Colleges & Universities Data Warehouse. We appreciate the efforts of the audit staff and their interest in working with us to improve our operations.

The Data Warehouse was initially created to respond to ad hoc requests for data. Demand for management information has continued to grow and the Warehouse currently serves as a critical resource for business operations and decisions. Since its functions have moved from ad hoc to essential services, ITS intends to incorporate the Data Warehouse into the standard IT functions and apply documented practices, procedures and security controls.

While we feel strongly that our current security infrastructure and policies provide a reasonable level of security for our systems and data, we plan to continue to enhance and improve our security policies, infrastructure and operations. The recommendations provided through this audit will help improve the data integrity, operations and security of the system for all users.

We look forward to ongoing communication with your staff as we work to resolve the issues raised in your audit findings.

Our response to address the current audit findings follows.

Sincerely,

/s/ Ken Niemi

Ken Niemi
Vice Chancellor for Information Technology & CIO

Finding 1: MnSCU has not documented existing procedures and has not developed formal standards and procedures for designing, testing and migrating the processes used to extract data from its source business systems.

Response:

- *Formal procedures will be implemented by the end of the fourth quarter of 2004. Our intent is to manage the warehouse reporting processes within the framework being established for all MnSCU software development efforts.*

Finding 2: MNSCU has not developed security policies, procedures, and standards for the data warehouse.

Response:

- *The Data Warehouse was initially created to respond to ad hoc requests for data. Over time, demand for various types of reports, both ad hoc and scheduled, continued to grow and are now considered essential to MnSCU core operations. ITS intends to incorporate the Data Warehouse into the standard IT functions, and apply documented practices, procedures and security controls. These standard IT functions will include access and server management procedures and controls, as well as a mechanism for periodically validating the adequacy of these controls. Transition planning is currently underway with a target turnover date during the fourth quarter of 2004. Unnecessary default network services and software on the warehouse servers have been removed, and all critical software patches have been installed. Further procedures for ensuring hardening of the servers will be implemented during the fourth quarter of 2004.*

Finding 3: One MnSCU employee performs many duties that are often considered incompatible.

Response:

- *ITS is implementing a new process to extract and load data into the warehouse. The majority of work related to the new process will fall on the operations and system management staff. Testing of the new process is expected to be completed by September 30, 2004. When implemented in the 4th quarter of 2004, these duties will have been separated between operations staff and data management staff will no longer have to be involved in the direct loading of data into the warehouse. In addition, the warehouse operations will be incorporated into the standard IT system management functions, with all duties appropriately segregated between operations and development staff during the 4th quarter of 2004.*