OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Department of Finance

Information Warehouse Data Integrity

As of May 2000

SEPTEMBER 15, 2000 **00-45**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota State government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately fifty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year and one best practices review.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of Representatives and Senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 651-296-1727 (voice), or the Minnesota Relay Service at 651-297-5353 or 1-800-627-3529.

All OLA reports are available at our Web Site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, evaluation, or best practices review, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

OLA

OFFICE OF THE LEGISLATIVE AUDITOR

State of Minnesota • James Nobles, Legislative Auditor

Representative Dan McElroy, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Ms. Pamela Wheelock, Commissioner
Department of Finance

We have conducted a financial-related audit of selected activities at the Minnesota Department of Finance. Our audit scope included a review of data integrity controls for the department's information warehouse as of May 2000.

We conducted our audit in accordance with *Government Audit Standard*s, 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 Department of Finance complied with the provisions of laws, regulations, contracts, and grants that are significant to the audit. The department's management 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 the Department of Finance. This restriction is not intended to limit the distribution of this report, which was released as a public document on September 15, 2000.

/s/ James R. Nobles	*/s/ Claudia J. Gudvangen*
James R. Nobles Legislative Auditor	Claudia J. Gudvangen, CPA Deputy Legislative Auditor

End of Fieldwork: May 30, 2000

Report Signed On: September 11, 2000

Department of Finance
Information Warehouse Data Integrity

Table of Contents

Audit Participation

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

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Christopher Buse, CPA, CISA	Audit Manager
Neal Dawson	Auditor-In-Charge
Eric Roggeman	Auditor

Exit Conference

We discussed the findings and recommendations of the audit with the following representatives of the Department of Finance on August 31, 2000:

Anne Barry	Deputy Commissioner
Jean Henning	Acting Chief Information Officer
Ellen Schwandt	Information Access Director

Report Summary

The Department of Finance has controls to ensure that information warehouse data is both accurate and complete. However, we identified several weaknesses that the department should address to improve its control structure.

Key Findings:

- Some accounts with extremely powerful security clearances have inadequate password controls. Also, several accounts with powerful security clearances were no longer needed. (Finding 1, page 6)

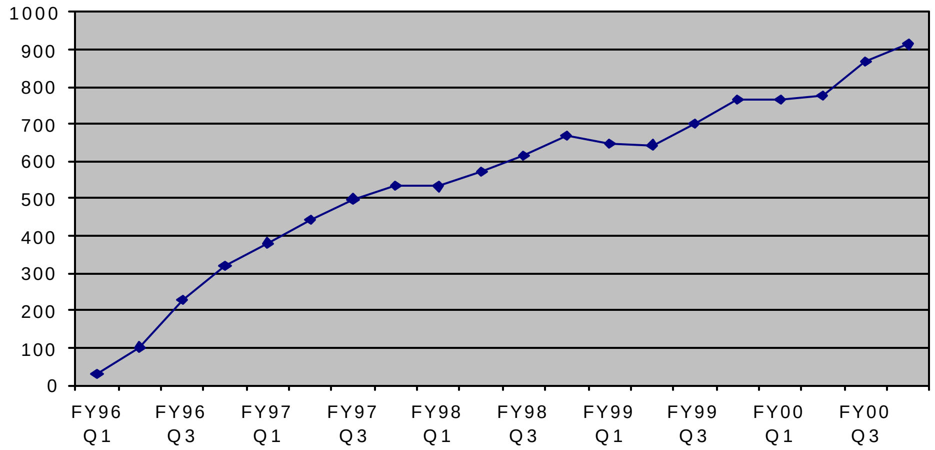
- Some information technology professionals may have more clearance than they need to fulfill their job duties. (Finding 2, page 7)

Chapter 1. Introduction

This audit analyzed how the Department of Finance controls the accuracy and completeness of data in its information warehouse. Controlling information warehouse data integrity is vital because state agencies use this system to support their daily business operations and make strategic planning decisions. In fact, many standard accounting, payroll, human resource, and budgeting reports have been eliminated because state agencies can now retrieve this same information from the warehouse.

The information warehouse began operations in 1995 with 20 users. As illustrated in Figure 1-1, the number of state agency employees who have queried information from the warehouse has steadily increased since that time. During May 2000, over 900 employees from 60 different state agencies retrieved data from the information warehouse.

Figure 1-1
Number of Employees Who Accessed the Information Warehouse
Fiscal Years 1996 through 2000

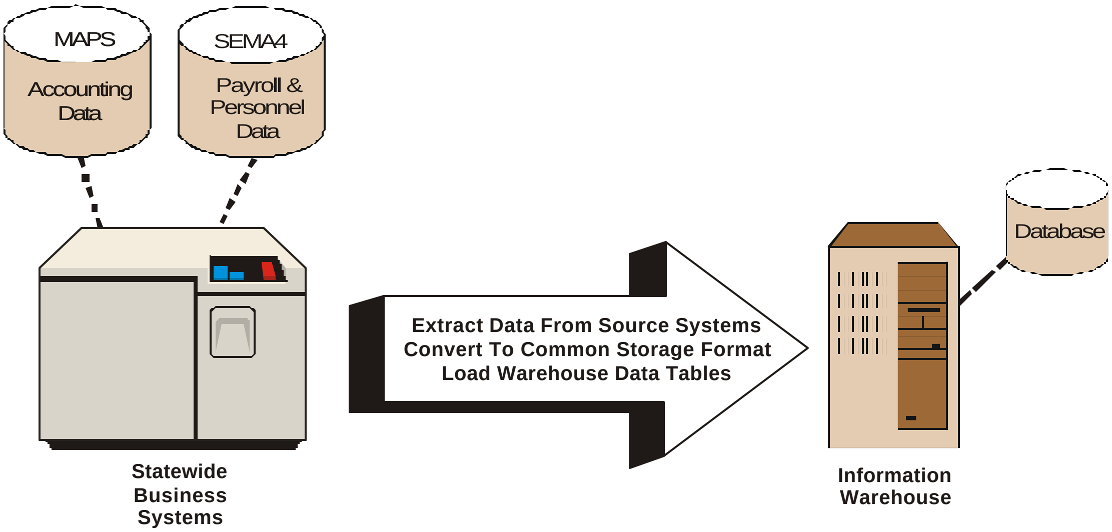


Source: Data provide by the Information Access Division.

The volume of data in the information warehouse has also increased to meet the diverse needs of state agencies. The number of database tables has grown from approximately 58 in 1995 to over 100 today. These tables now contain over 200 million rows of data.

The tables in the information warehouse contain a vast array of accounting, budgeting, payroll, and personnel data. The department obtains this data from the Minnesota Accounting and Procurement System (MAPS) and the statewide payroll and personnel system (SEMA4). As depicted in Figure 1-2, the department extracts the data from these systems, converts it to a consistent storage format, and loads the information warehouse tables.

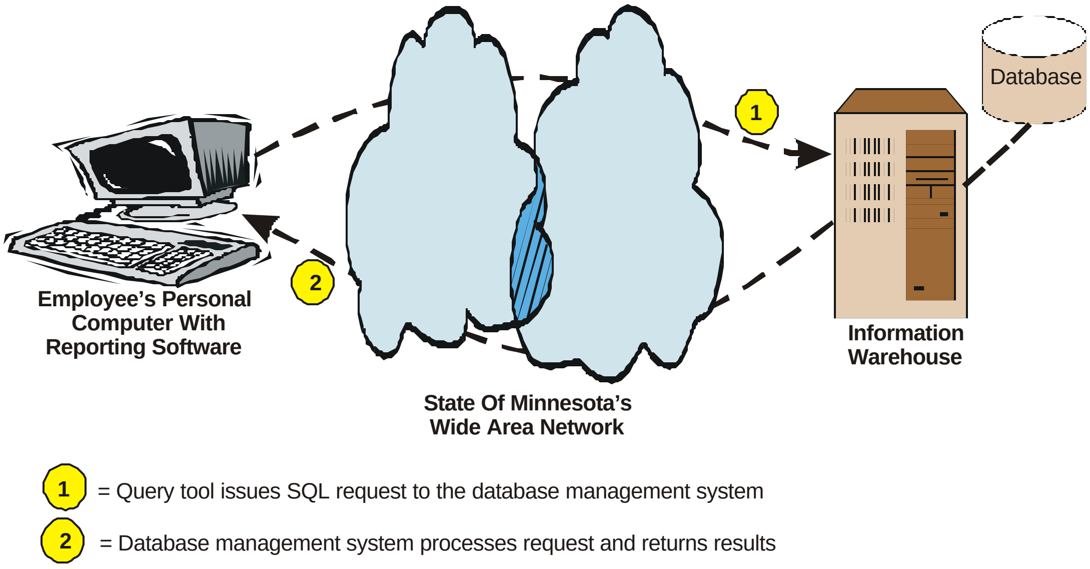
Figure 1-2
Populating Information Warehouse Data Tables


MAPS
Accounting Data
SEMA4
Payroll & Personnel Data
Statewide Business Systems
Extract Data From Source Systems
Convert To Common Storage Format
Load Warehouse Data Tables
Database
Information Warehouse

Source: Auditor prepared.

Employees in state agencies use reporting software, such as Seagate Crystal Reports or Microsoft Access, to retrieve information from the warehouse. As illustrated in Figure 1-3, these reporting programs locate the computer that houses the information warehouse and establish a connection to its database management system. The programs then issue a request for data, written in a special language called Structured Query Language (SQL). The database management system processes these requests and returns the results.

Figure 1-3
Querying Information Warehouse Data


Employee's Personal Computer With Reporting Software
State Of Minnesota's Wide Area Network
1
2
Database
Information Warehouse
1 = Query tool issues SQL request to the database management system
2 = Database management system processes request and returns results

Source: Auditor prepared.

The information warehouse resides on a powerful computer that is located in the Department of Administration's Intertech data center. The AIX operating system running on this computer is a UNIX-based operating system that was developed by International Business Machines. Oracle Corporation developed the database management system installed on this machine. The department uses both AIX and Oracle security features to control access to the information warehouse data.

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 statewide business systems and the information warehouse. Chapter 2 discusses the scope of our work and the conclusions that we reached.

Chapter 2. Warehouse Data Integrity Controls

Chapter Conclusions

The Department of Finance has controls to ensure that information warehouse data is both accurate and complete. However, we found several weaknesses that the department should address to improve its control structure:

- ***Some accounts with extremely powerful security clearances have inadequate password controls.***
- ***Several accounts with powerful security clearances were no longer needed.***
- ***Some information technology professionals may have more clearance than they need to fulfill their job duties.***

Data integrity controls are those controls that help ensure both the accuracy and completeness of data. In an information-warehousing environment, processes used to load data tables need well-defined integrity controls. Those controls help ensure that data copied to the warehouse is identical to the same data found in the production business systems, such as the Minnesota Accounting and Procurement System. Data also must be tightly secured once in the warehouse. Strong security controls help protect data from losing its integrity through unauthorized changes. Finally, in some cases, information system professionals must correct data errors in production business systems. When this occurs, organizations need controls to synchronize data maintenance between its production business systems and its information warehouse. Without synchronization, production business system data fixes could lead to a gradual degradation of information warehouse data integrity.

Audit Objectives and Methodology

We designed our work to answer the following three questions:

- Does the department have procedures to ensure that the data transferred to the warehouse is accurate and complete?
- Does the department have appropriate security administration procedures to prevent unauthorized changes to warehouse data?
- Does the department have controls to ensure that data maintenance is synchronized between production business systems and the information warehouse?

To answer these questions, we interviewed the information system professionals in the Department of Finance who managed the warehouse and designed its data integrity controls. We also analyzed security data from both the AIX operating system and the Oracle database management system.

Conclusion

The Department of Finance has adequate data integrity controls for its information warehouse. The department has controls to ensure that the data transferred to the warehouse is both accurate and complete. The department also has controls to prevent unauthorized changes to warehouse data. Finally, the department has controls to synchronize data maintenance between production business systems and the information warehouse.

Though overall data integrity controls were satisfactory, our audit identified several issues that the department needs to address. We found some accounts with extremely powerful security clearances that had inadequate password controls. We also found several powerful accounts that were no longer needed. Finding 1 discusses these issues in more detail. As discussed in Finding 2, our audit identified some information system professionals in the Department of Finance who may have more clearance than they need to fulfill their job duties.

1. The information warehouse contains some powerful accounts with inadequate password controls and other accounts that are no longer needed.

The department did not enforce industry standard password controls for some of its most powerful accounts. Also, the department did not delete some powerful accounts that were no longer needed. These account and password administration weaknesses expose the information warehouse data to unnecessary risks.

We examined password controls for powerful accounts with clearance to the AIX operating system and the Oracle database management system. Information system professionals frequently need this level of clearance to manage the computer's hardware and software. On average, we found that passwords for these powerful accounts had not been changed for over 300 days. Security features that come standard with the AIX operating system and Oracle could force people to change their passwords after a certain number of days. They also could force people to select passwords that are difficult to guess. However, the department did not use these control features. Computer hackers often use password guessing programs to gain access to computer systems. Forcing people to select complex passwords and periodically change those passwords helps protect computer systems from these unscrupulous individuals.

We also tested two special software accounts that had extremely powerful security clearances. Manufacturers strongly encourage information system professionals to change the default passwords for software accounts after installing their products. However, using commonly known default passwords, we were able to access both the AIX operating system and the Oracle database management system. After our review, information system professionals in the department changed the default passwords on these unprotected accounts.

Finally, we found two obsolete software accounts with extremely powerful security clearances. When questioned, information system professionals told us that they used these accounts to evaluate several software packages. However, they did not remove them after completing the evaluation.

Recommendations

- *The department should force people with powerful security clearances to select complex passwords and change those passwords frequently.*
- *The department should immediately change the default passwords for new software accounts.*
- *The department should remove or disable any unnecessary accounts.*

2. Some information technology professionals have excessive security clearances.

Some information technology professionals have broader security clearances than they need to fulfill their job duties. We found four information technology professionals with clearance in Oracle to run any program, including those used to update data in information warehouse tables. When questioned, the department could not justify why these employees needed such broad security clearances.

Granting people more access than they need to fulfill their typical job duties creates an unnecessary security risk. To improve controls, the department should define security clearances for each of its information technology professionals that is appropriate for their job duties.

Recommendation

- *The department should only give employees the security clearance that they need to fulfill their normal job duties.*

State of Minnesota
Department of Finance

400 Centennial Building
658 Cedar Street
St. Paul, Minnesota 55155
Voice: (651) 296-5900
Fax: (651) 296-8685
TTY: 1-800-627-3529

September 7, 2000

James R. Nobles
Legislative Auditor
Office of the Legislative Auditor
1st Floor South-Centennial Building
658 Cedar Street
St. Paul, Minnesota 55155

Dear Mr. Nobles:

Thank you for the opportunity for my staff to discuss your audit findings with the people in your office responsible for the Department of Finance audit. We are pleased with your audit conclusions that indicate our information warehouse has strong data integrity controls that ensure warehouse data is both accurate and complete. As you are aware, we are committed to providing accurate financial information to state agencies, the legislature, and the public. We will continue to work toward improvements in our data integrity controls for the department's information warehouse by addressing the minor findings contained in your audit report.

Recommendation

The department should force people with powerful security clearances to select complex passwords and change those passwords frequently.

Response

The Department of Finance will develop and implement password change routines that require use of complex passwords and frequent password changes.

Person Responsible: Ellen Schwandt, Director, Information Access Unit

Estimated Completion date: December 31, 2000

Recommendation

The department should immediately change the default passwords for new software accounts.

Response

The default passwords on the two accounts identified have been changed. In the future, default passwords will be changed at installation.

Recommendation

The department should remove or disable any unnecessary accounts.

Response

The two accounts identified have been removed. In the future, when an account is identified as no longer necessary, it will be promptly removed.

Recommendation

The department should only give employees the security clearances that they need to fulfill their normal job duties.

Response

The Oracle security for four information technology professionals has been modified to restrict which programs they are able to execute. All Oracle and AIX clearances have been reviewed and no other changes are planned.

We appreciate the opportunity to participate in such reviews of our systems by your organization and your recommendations on how to further strengthen the strict controls we have implemented to protect our information warehouse operation.

Sincerely,

/s/ Pamela Wheelock

Pamela Wheelock
Commissioner