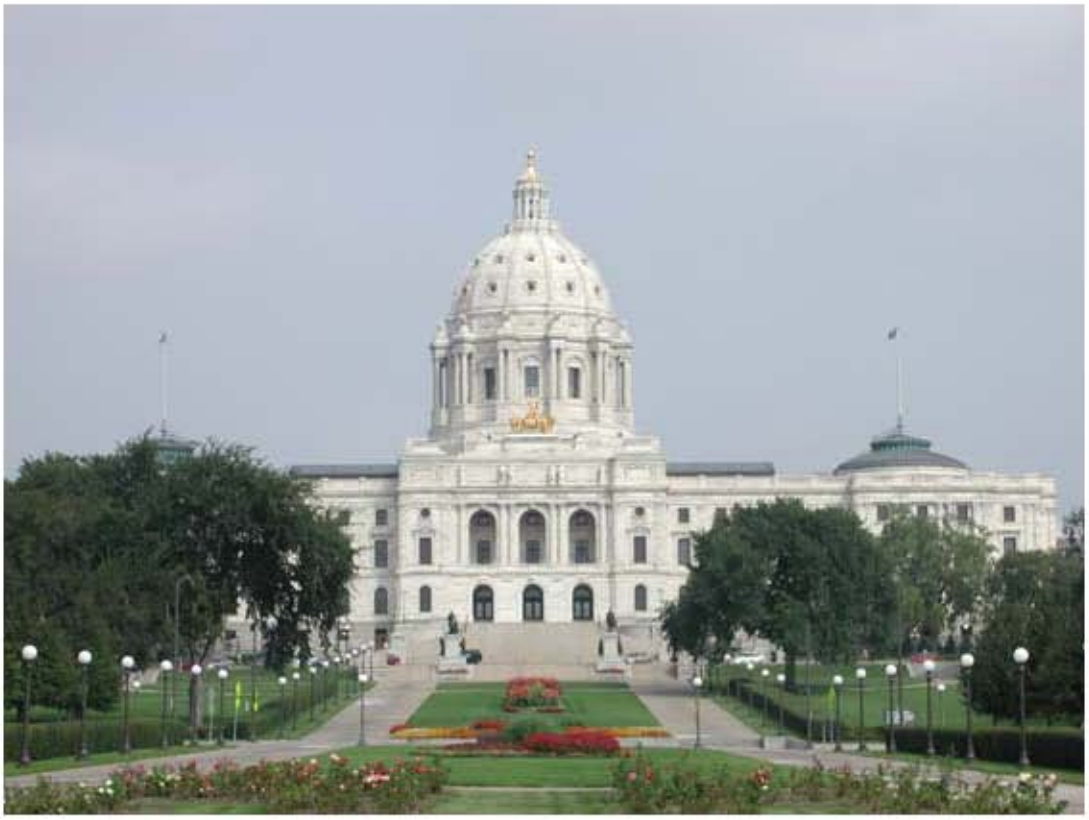
O L A

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Department of Finance

Information Warehouse Integrity and Confidentiality Controls



December 13, 2007 **07-34**

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.

To obtain a copy of this document in an accessible format (electronic ASCII text, Braille, large print, or audio) please call 651-296-1235. People with hearing or speech disabilities may call us through Minnesota Relay by dialing 7-1-1 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

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

Financial Audit Division Report

Department of Finance

Information Warehouse Integrity and Confidentiality Controls

December 13, 2007 **07-34**

FINANCIAL AUDIT DIVISION
Centennial Building – Suite 140
658 Cedar Street – Saint Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web site: http:/www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

OLA

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

Representative Rick Hansen, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Tom Hanson, Commissioner
Minnesota Department of Finance

We have conducted an information technology audit of the information warehouse. The audit focused on the department's controls that help to protect the integrity and confidentiality of its data. The Report Summary highlights our overall conclusion. Our specific audit objective and conclusions are contained in Chapter 2 of this report. The report contains three findings related to security weaknesses.

We would like to thank the staff from the Department of Finance for their cooperation during this audit.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Cecile M. Ferkul

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

End of Fieldwork: August 31, 2007

Report Signed On: December 10, 2007

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Table of Contents

	Page
Report Summary	1
Chapter 1. Introduction	2
Chapter 2. Data Integrity and Confidentiality Controls	3
Status of Prior Audit Issues	6
Agency Response	7

Audit Participation

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

Cecile Ferkul, CPA, CISA	Deputy Legislative Auditor
Eric Wion, CPA, CISA, CISSP	Audit Manager
John Kelcher	Auditor-in-Charge
Bill Betthauser	Auditor
Mike Woolley, CISA, CISSP	Auditor

Exit Conference

We discussed the findings and recommendations with the following representatives of the Department of Finance and the Office of Enterprise Technology at the exit conference held November 29, 2007:

Department of Finance:

Tom Hanson	Commissioner
Stephanie Andrews	Deputy Commissioner
Steve Jorgenson	Chief Information Officer
Jean Henning	Chief Technology Officer
Ellen Schwandt	Information Access Director
Bob Dockendorf	Technical Services Director

Department of Employee Relations:

Andre Drinkwine	Technical Services Supervisor

Office of Enterprise Technology:

Mark Mathison	IT Compliance Audit Manager

Department of Finance
Information Warehouse Integrity and Confidentiality Controls

Report Summary

Conclusion:

The Department of Finance generally had adequate controls to protect the integrity and confidentiality of its data in the information warehouse. However, the department had some security weaknesses.

Findings:

- The department had few written policies, standards, and procedures for securing the information warehouse. (Finding 1, page 4)
- The department did not always enforce strong password controls. (Finding 2, page 4)
- The department did not develop comprehensive security monitoring procedures. (Finding 3, page 5)

Audit Scope:

We assessed the department's controls to protect the integrity and confidentiality of its information warehouse data as of August 2007.

Background:

The Department of Finance manages the state's information warehouse. The warehouse is a very large data repository containing over one billion rows of current and historical accounting, procurement, payroll, and personnel data. State agencies use this data to monitor their operations, perform financial analysis, and compile data for internal and external reports. In addition, the Department of Finance uses the warehouse to help prepare the state's Comprehensive Annual Financial Report. The warehouse has over 2,000 users.

Chapter 1. Introduction

The Department of Finance manages the state's information warehouse. The warehouse is a very large data repository containing over one billion rows of current and historical accounting, procurement, payroll, and personnel data. State agencies use this data to monitor their operations, perform financial analysis, and compile data for internal and external reports. In addition, the Department of Finance uses the warehouse to help prepare the state's Comprehensive Annual Financial Report. The warehouse has over 2,000 users who access the data through a variety of reporting software programs.

This information technology audit assessed the adequacy of the department's controls to protect the integrity and confidentiality of the data in its information warehouse.

Audit Approach

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We used guidance contained in the *Control Objectives for Information and Related Technology (COBIT)* and *ISO/IEC 17799* as our criteria to evaluate controls.[1] We also used the Department of Finance's policies and procedures to obtain evaluation criteria. Finally, we used information published by applicable technology vendors to evaluate select controls.

[1] COBIT, published by the IT Governance Institute, is an IT governance framework providing organizations with a set of generally accepted measures, indicators, processes, and best practices to assist them in developing appropriate IT governance and control in an organization. ISO/IEC 17799 is an international information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Chapter 2. Data Integrity and Confidentiality Controls

Chapter Conclusions

The Department of Finance generally had adequate controls to protect the integrity and confidentiality of its information warehouse data. However, the department had some security weaknesses. The department had few written policies, standards, and procedures for securing the data warehouse. In addition, it did not always enforce strong password controls, and it had not developed comprehensive security monitoring procedures.

Data integrity controls help ensure data is complete and accurate. Well-defined data integrity controls help ensure that data copied to the warehouse is identical to the data found in the production business systems, including the Minnesota Accounting and Procurement System and the State Employee Management System. These controls also ensure that data remains secured once in the warehouse. For example, strong security controls help protect data from unauthorized changes. In addition, synchronization controls ensure that the department corrects warehoused data whenever it makes corrections to the production business systems. Without synchronization, production business system data fixes could lead to a gradual degradation of warehouse data integrity.

Confidentiality controls help ensure that sensitive data, such as social security numbers, cannot be seen by unauthorized individuals. Strong security controls help protect data from unauthorized disclosure.

Audit Objective

Our review of controls focused on the following question:

- Did the department have adequate controls to protect the integrity and confidentiality of its information warehouse data?

The department had the following weaknesses in its data integrity and data confidentiality controls:

Current Findings and Recommendations

1. The department had few written policies, standards, and procedures for securing the data warehouse.

The department had few written security policies, standards, and procedures. It is vital that the department document this information because it provides the department's information technology staff 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.

Recommendation

- *The department should develop security-related policies, standards, and procedures.*

2. The department did not always enforce strong password controls.

The department did not always enforce strong password controls for all of its data warehouse accounts. Strong password controls are critical because they help prevent unauthorized people from assuming the identity of legitimate system users to gain access to computer systems and data.

The software products used by the information warehouse have customizable features to enforce strong password controls. For example, the software products allow the department to enable features that prevent users from selecting easy to guess passwords, like dictionary words, and require passwords to be periodically changed. In addition, the software products allow the department to automatically disable accounts if excessive failed login attempts occurred. The department did not always customize the software products to put these types of controls in place.

Recommendation

- *The department should enforce strong password controls.*

3. The department did not develop comprehensive security monitoring procedures.

The department did not fully assess its risks to determine which security events required logging, who should review them, and how timely they need review. While the software products used by the information warehouse had customizable features that allow events to be logged, the department logged few events. In addition, it did not routinely review some logged events. Consequently, the department may not be able to promptly identify and respond to signs of potential security breaches or system misuse until significant damage has occurred.

Recommendation

- *The department should assess its risks and define specific security-related events to log, who should review them, and the timeliness of the reviews.*

Status of Prior Audit Issues
As of August 31, 2007

Most Recent Audit Report 04-07, issued in February 2004, did not contain any findings or recommendations for improvement. The audit scope included the information warehouse's data integrity controls.

State of Minnesota Audit Follow-Up Process

The Department of Finance, on behalf of the Governor, maintains a quarterly process for following up on issues cited in financial audit reports issued by the Legislative Auditor. The process consists of an exchange of written correspondence that documents the status of audit findings. The follow-up process continues until Finance is satisfied that the issues have been resolved. It covers entities headed by gubernatorial appointees, including most state agencies, boards, commissions, and Minnesota state colleges and universities. It is not applied to audits of the University of Minnesota, any quasi-state organizations, such as metropolitan agencies or the State Agricultural Society, the state constitutional officers, or the judicial branch.

MINNESOTA DEPARTMENT OF FINANCE

December 7, 2007

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street
140 Centennial Office Building
St. Paul, MN 55155-4708

Dear Mr. Nobles:

Thank you for the opportunity for our staff to discuss your audit finding with the individuals in your office responsible for the Information Access Data Warehouse audit. We are committed to providing secure access to accurate, timely data to state agencies, the legislature and the public. We also are thankful for the written and verbal reviews by the team that performed this work from your office. At the exit conference, we were pleased to hear that the security work we have done with our applications ranks among the best they have seen in state government. We know that there is always more to do and that security is an ever-changing and ever-challenging issue. We remain committed to providing excellent security, and we will continue to work toward improvements in our processes.

Finding 1: The department had few written policies, standards, and procedures for securing the data warehouse.

Recommendation: The department should develop security-related policies, standards, and procedures.

Response: We concur with the recommendation. While the Department of Finance practices sound security practices and procedures, it does not have a written set of security policies, standards and procedures that document these practices. Security-related policies, standards and procedures for securing the IA Data Warehouse will be written.

Person responsible: Ellen Schwandt, Director, Information Access
Implementation date: December 2008

Finding 2: The department did not always enforce strong password controls.

Recommendation: The department should enforce strong password controls.

Response: We concur with the recommendation. While the Department of Finance uses system features to enforce strong password controls on user accounts; on some non-user accounts strong password controls are enforced without the use of customized software products. The Department of Finance will review, customize and implement the use of software products to enforce strong password controls for additional IA Data Warehouse accounts.

400 Centennial Building • 658 Cedar Street • St. Paul, Minnesota 55155
Voice: (651) 201-8000 • Fax: (651) 296-8685 • TTY: 1-800-627-3529
An Equal Opportunity Employer

Person Responsible: Ellen Schwandt, Director, Information Access
Implementation Date: June 2008

Finding 3: The department did not develop comprehensive security monitoring procedures.

Recommendation: The department should assess its risks and define specific security-related events to log, who should review them, and the timeliness of reviews.

Response: We concur with the recommendation. The Department of Finance will assess its risks and define specific security-related events to log, who should review the logs, and the timeliness of reviews. It will implement identified logging and monitoring.

Person Responsible: Ellen Schwandt, Director, Information Access
Implementation Date: December 2008

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,

Tom J Hanson

Tom Hanson
Commissioner