OLA **OFFICE OF THE LEGISLATIVE AUDITOR**
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

State Board of Investment

Information Technology Audit

August 13, 2009 **Report 09-26**

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

Financial Audit Division

The 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 has a staff of 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.

The Office of the Legislative Auditor (OLA) also has a Program Evaluation Division, which evaluates topics periodically selected by the Legislative Audit Commission.

Reports issued by both OLA divisions are solely the responsibility of OLA and may not reflect the views of the Legislative Audit Commission, its individual members, or other members of the Minnesota Legislature. For more information about OLA reports, go to:

http://www.auditor.leg.state.mn.us

To obtain reports in electronic ASCII text, Braille, large print, or audio, call 651-296-4708. People with hearing or speech disabilities may call through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

To offer comments about our work or suggest an audit, investigation, or evaluation, call 651-296-4708 or e-mail auditor@state.mn.us.

OLA

OFFICE OF THE LEGISLATIVE AUDITOR

State of Minnesota • James Nobles, Legislative Auditor

August 13, 2009

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Howard Bicker, Executive Director
State Board of Investment

This report presents the results of our information technology audit of the State Board of Investment's (SBI) controls. The scope of our audit focused on controls that help to protect the integrity, confidentiality, and availability of SBI's computer systems and business data. This report contains two findings presented in the accompanying section of this report titled, *Findings and Recommendations*.

We discussed the results of the audit with SBI on July 29, 2009. SBI's response to our findings and recommendations is presented in the accompanying section of this report titled, *Agency Response.*

The audit was conducted by Eric Wion (Audit Manager) and Bill Betthauser (Auditor-in-Charge).

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Cecile M. Ferkul

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Table of Contents

Page

Report Summary 1

Agency Overview 3

Objectives, Scope, and Methodology 3

Conclusion 4

Findings and Recommendations 5

1. SBI lacked important security documentation...................................5

2. SBI did not sufficiently maintain or monitor some aspects of its computer network 5

Agency Response..7

Report Summary

Conclusion

The State Board of Investment (SBI) generally had adequate controls to protect the confidentiality, integrity, and availability of its computer systems and data. However, we found two weaknesses in internal controls.

Findings

- SBI lacked important security documentation. (Finding 1, page 5)

- SBI did not sufficiently maintain or monitor some aspects of its computer network. (Finding 2, page 5)

Audit Objective and Scope

The audit objective was to answer the following question:

- Did SBI have adequate controls to protect the confidentiality, integrity, and availability of its computer systems and business data?

We assessed controls as of July 2009.

State Board of Investment

Agency Overview

The State Board of Investment (SBI) develops and implements investment policies and strategies for the state's retirement funds, trust funds, and cash accounts. The statutory mission of the SBI is to establish standards that will ensure that state and pension assets will be responsibly invested to maximize the total rate of return without incurring undue risk.[1] SBI uses both internal staff and external money managers to fulfill its responsibilities. The external firms invest and manage the assets of the retirement funds and the assigned risk plan, while internal staff manages other state investments.

SBI manages a relatively simple computing environment. The risk of data tampering or disclosure is low. Its computing environment does not consist of any internal business applications. For example, the investment trade activity occurs on external third-party computer systems and not SBI's. Generally, SBI does not maintain not public data.

Objective, Scope, and Methodology

The audit objective was to answer the following question:

- Did SBI have adequate controls to protect the integrity, confidentiality, and availability of its computer systems and business data?

To answer this question, we interviewed SBI staff and reviewed other relevant documentation. We also used a variety of computer-assisted auditing tools and other techniques to analyze the security infrastructure.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To assess security controls, we used criteria contained in the *Control Objectives for Information and Related Technology (COBIT*), published by the IT Governance Institute.[2] We also used criteria obtained in security guidance published by the National Institute of Standards and Technology's Computer Security Division, the National Security

[1] *Minnesota Statutes* 2008, 11A.01.

[2] COBIT 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.

Agency, and the Defense Information Systems Agency. Finally, we used information published by applicable technology vendors to evaluate select controls.

Conclusion

SBI generally had adequate controls to protect the integrity, confidentiality, and availability of its computer systems and business data. However, we found two weaknesses in internal controls.

The following *Findings and Recommendations* section explains the deficiencies.

Findings and Recommendations

Finding 1

SBI lacked important security documentation.

SBI lacked important security documentation, such as risk assessments, policies, standards, and procedures. Formal risk assessments are important because they help to identify information security risks, determine the appropriate management action and priorities for managing those risks, and document controls selected to protect against risks. Policies, standards, and procedures are important because they outline management's security decisions and methods to implement them.

Recommendation

- *SBI should document its important security decisions, including policies, standards, procedures, and risk assessments.*

Finding 2

SBI did not sufficiently maintain or monitor some aspects of its computer network.

SBI had the following weaknesses related to maintaining and monitoring its network:

- SBI did not promptly install software updates or security-related software patches on some of its computers. Computer hackers routinely discover and exploit flaws in commercial software to gain unauthorized access to computer systems. When these exploits occur, vendors develop and publish software patches to correct the deficiencies in their products. Agencies that do not promptly install these software patches make their systems easy targets for computer hackers. Staying up to date with software patches can be a very challenging task for an organization. To meet this challenge, organizations need a formal process to learn about new vulnerabilities and determine whether their systems are at risk.

- SBI did not filter or restrict internal traffic leaving the private network to the Internet to ensure only authorized computer activity was allowed.[3] In addition, it did not filter traffic between itself and the few third parties with whom it had private dedicated computer connections. These connections allowed each party to access one another's computer systems.

[3] SBI did adequately filter or restrict computer traffic originating from the Internet and passing into its internal private network.

Although the connections were private, they allowed any computer traffic to or from SBI.

- It did not develop monitoring procedures to detect and promptly respond to security-related events. In addition to external attacks, such as unauthorized attempts to access computers, other events may require monitoring, such as system misuse by employees, changes to critical computer settings, and exceptions to defined policies and procedures.

Recommendations

- *SBI should install software updates in a timely manner.*

- *SBI should filter Internet-bound internal traffic and the computer traffic between itself and third parties to ensure only authorized computer activities occur.*

- *SBI should assess its risks, define specific events to log, and designate who should review those events and the frequency of the review.*

MINNESOTA
STATE
BOARD OF
INVESTMENT

60 Empire Drive
Suite 355
St. Paul, MN 55103
(651) 296-3328
FAX (651) 296-9572
E-mail:
minn.sbi@state.mn.us
www.sbi.state.mn.us

An Equal Opportunity Employer

August 5, 2009

Mr. James R. Nobles
Legislative Auditor
Office of the Legislative Auditor
Room 140 Centennial Building
658 Cedar Street
St. Paul, Minnesota 55155

Dear Mr. Nobles:

Thank you for the opportunity to respond to the information technology (IT) audit you conducted at the State Board of Investment (SBI).

Finding 1: SBI lacked important security documentation.

Audit Recommendation: SBI should document its important security decisions, including policies, standards, procedures, and risk assessments.

Audit Response: The SBI agrees with the finding that some of the security documentation is lacking and acknowledges the importance of such documentation.

The SBI will continue to develop and maintain security documentation within the constraints of its IT resources.

The SBI understands that the Office of Enterprise Technology (OET) is working on a template that will assist agencies in documenting policies, standards, procedures and risk assessments. The SBI endorses this effort and believes this would aid the SBI and other agencies in their security documentation.

Person Responsible: Kathy Leisz

Implementation Date: June 30, 2011

Finding 2: SBI did not sufficiently maintain or monitor some aspects of its computer network.

Audit Recommendations:

- SBI should install software updates in a timely manner.
- SBI should filter Internet-bound internal traffic and the computer traffic between itself and third parties to ensure only authorized computer activities occur.
- SBI should assess its risks, define specific events to log, and designate who should review those events and the frequency of the review.

Audit Response: The SBI acknowledges the importance of installing software updates in a timely manner. While most updates have been completed in a timely manner, the SBI will strive to improve in the timeliness of installing updates.

The SBI will evaluate the filtering of Internet-bound traffic and the computer traffic between itself and third parties to ensure only authorized computer activities occur and implement such filters as deemed appropriate. The SBI will also assess its risks and determine what events should be logged and then review the logs in a timely and organized fashion.

Person Responsible: Kathy Leisz

Implementation Date: Ongoing

Thank you for the recommendations you have made to improve the security of the SBI computer systems and data, and for the constructive discussions we have had with your staff.

Sincerely,

/s/ Howard Bicker

Howard Bicker
Executive Director