OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Revenue

GenTax

Information Technology Security Controls

February 28, 2013 **Report 13-04**

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

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

February 28, 2013

Senator Roger Reinert, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Myron Frans, Commissioner
Department of Revenue

This report presents the results of our information technology security audit of the Department of Revenue's integrated tax system, GenTax. The audit examined how well the department protected GenTax and the underlying databases from unauthorized changes and viewing. We assessed the department's controls as of November 2012.

The audit was conducted by Carolyn Engstrom, CPA, CISA (IT Audit Manager), David Westlund, CPA, CISA (IT Senior Auditor), and assisted by Thom Derus (IT Auditor).

We received the full cooperation of the Department of Revenue while performing this audit.

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Phone: 651-296-4708 • Fax: 651-296-4712
E-mail: legislative.auditor@state.mn.us • Web Site: www.auditor.leg.state.mn.us • Minnesota Relay: 1-800-627-3529 or 7-1-1

Table of Contents

Report Summary

Conclusion

The Department of Revenue generally had adequate internal controls to ensure that it protected databases containing tax-related information from unauthorized modification and viewing and to ensure that changes made to GenTax and its supporting infrastructure were authorized. However, the department had the following internal control deficiencies:

Findings

- The Department of Revenue had not completed some elements of a comprehensive security plan for GenTax, as required by its standard. (Finding 1, page 7)
- The Department of Revenue did not adequately monitor changes to GenTax and its supporting infrastructure to ensure they complied with the department's plan. (Finding 2, page 8)
- The Department of Revenue had not clearly documented expectations for its review of reports that tracked changes to or viewing of data within the database or changes to the database structure. (Finding 3, page 9)
- The Department of Revenue had not implemented adequate controls to prevent and detect some inappropriate access to servers and databases supporting GenTax. (Finding 4, page 10)
- The Department of Revenue had not finalized its documentation of security configuration baseline standards for infrastructure supporting GenTax. (Finding 5, page 11)

Audit Objective and Scope

The audit objective was to determine whether the Department of Revenue had adequate information technology controls, as of November 2012, to protect databases containing taxpayer information from unauthorized modification or viewing and to ensure that changes made to GenTax and its supporting infrastructure were authorized.

Department of Revenue

Information Technology Security Controls

Overview

In 2007, the Department of Revenue purchased GenTax, an integrated tax processing software developed by Fast Enterprises. When implementation was completed in February 2012, GenTax replaced over 30 applications and many supporting tools, databases, and interfaces the department had used to collect data and tax receipts. From February 2012 through February 2013, the software was in the "warranty and stabilization" phase, during which the department focused on optimizing GenTax's efficiency and effectiveness. The department estimated the total cost of the project, including hardware, software, and internal resources, was about $40 million, including about $26 million paid to Fast Enterprises for GenTax through January 28, 2013. As of November 2012, about 130 information technology staff and 8 contractors supported the department's technology processing environment, which included about 55 Web, database, and application servers that support GenTax.

GenTax processed tax revenue totaling about $16 billion in fiscal year 2012, including corporate income, individual income, state sales, property, and other taxes. Because of the significant financial activity GenTax processes and the substantial amounts and types of data about the state's citizens and taxpayers in GenTax's databases, internal controls to protect data integrity and privacy are critical.[1] Through GenTax the department can limit an employee's ability to modify and view data to the needs of an employee's work assignment. GenTax also allows the department to restrict the records an employee can view and can log the records each employee does view.

As with any software application, the department also has information technology employees and contractors who need to manage the hardware and databases to ensure GenTax operates as intended. To perform their jobs, these employees and contractors have access to the hardware and databases that is not controlled by GenTax but by its supporting operating systems and database management systems. This extensive access granted to information technology employees and contractors required to perform their job duties also creates a risk of unauthorized changes and viewing of data.

[1] The federal Internal Revenue Service (IRS) requires the state to have data security standards to protect federal tax information as if the information remained in IRS's hands. IRS Publication 1075*, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities*, contains specific requirements for safeguarding federal tax information. While these requirements satisfy the expectations of the federal government for federal tax data, they may not be sufficient to satisfy state officials about data protection expectations for all the department's tax information.

Initially, the department relied on its information technology employees and contractors to support the development of GenTax and its information technology infrastructure. In 2011, when the state consolidated its information technology services, most of the department's information technology employees became employees of the state's Office of Enterprise Technology.[2] These employees now report to the state's chief information officer, and the department obtains its information technology services through an interagency agreement with the Office of Enterprise Technology. Many of the Office of Enterprise Technology employees providing those services formerly provided the same services as Department of Revenue employees.

The information technology consolidation provided the state with the opportunity to more effectively and economically protect data held by the state. However, one challenge resulting from the consolidation is delineating the shared responsibility for the security of the state's computer systems and the protection of data in the state's databases. State statutes require each state agency to "establish appropriate security safeguards for all records containing data on individuals"[3] and to notify individuals if any breach of security occurs.[4] On the other hand, departments need to rely on information technology staff of the Office of Enterprise Technology for the technical expertise required to understand and assess the risks related to data protection. State statutes describe the Office of Enterprise Technology's responsibility for protection of state data and systems as more than that of a "service provider;" rather, the office is to "ensure overall security of the state's information and technology systems and services."[5] To fulfill this responsibility, the office will need to collaborate with department management to understand the wide range of operational needs and risks that can affect security decisions.

Objective, Scope, and Methodology

The audit objective was to answer the following questions, as of November 2012:

- Did the Department of Revenue have adequate information technology security controls to protect databases containing taxpayer information from unauthorized modification or viewing?

- Did the Department of Revenue have adequate controls to ensure that changes made to GenTax and its supporting infrastructure were authorized?

[2] The Office of Enterprise Technology refers to itself as Mn.IT Services.
[3] *Minnesota Statutes* 2012, 13.05, subd. 5.
[4] *Minnesota Statutes* 2012, 13.055, subd. 2.
[5] *Minnesota Statutes* 2012, 16E.01, subd. 3 (14).

To answer these questions, we interviewed information technology staff and contractors and reviewed relevant documentation. We also used a variety of computer-assisted auditing tools and other techniques to analyze the system's security and test controls. We assessed the effectiveness of the following internal controls:

- Access controls – Were the department's password policies and other authentication mechanisms effective to appropriately restrict users' access? Were users given only the access they needed to perform their job duties? Were certain incompatible duties segregated? If not, did the department have appropriate monitoring in place to ensure that transactions were accurate and authorized?

- Change management controls – Did the department document its expectations for system settings? Were changes to the system requested, tested, and authorized? Were changes to the system monitored to detect unauthorized changes?

- Report integrity – Were GenTax reports that were used to record financial data into the state's accounting system accurate and complete?

- Operations controls – Were automated processing jobs appropriately scheduled and monitored?

- Vulnerability management – Were vulnerabilities identified, analyzed, and mitigated?

We did not test whether employees with authorized access through the department's tax system (GenTax) used that access to modify or view tax information beyond the needs of their work assignments.

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 Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, published by the National Institute of Standards and Technology's Computer Security Division. When available, we also used department and state policies to obtain evaluation criteria. We also used criteria contained in security guidance, published by the Defense Information Systems Agency, and information published by applicable technology vendors to evaluate select controls.

Conclusion

The Department of Revenue generally had adequate internal controls to ensure that it protected databases containing tax-related information from unauthorized

modification and viewing and to ensure that changes made to GenTax and its supporting infrastructure were authorized. However, the department had some internal control deficiencies, as explained in the Findings and Recommendations section of this report.

We addressed the findings and recommendations in this report to the management of the Department of Revenue. However, they will need to work in consultation and coordination with the Office of Enterprise Technology to resolve the internal control weaknesses.

Findings and Recommendations

Finding 1

The Department of Revenue had not completed some elements of a comprehensive security plan for GenTax, as required by its standard.

The department did not complete some elements required by its standard for a comprehensive security plan.[6] Table 1 shows the elements required by the department's security plan standard and identifies whether the department had documentation for the requirement related to GenTax and its supporting servers and databases.

Table 1
Department of Revenue
Security Plan Requirements and Documentation

Required Element of Security Plan	Documentation for GenTax?
Project, Purpose, and Overview	Yes
Architecture Diagram	Yes
Access Authorization Matrix	Partially
Data Classification	Partially
Standards Compliance	Partially
Security Exceptions, Risks, and Mitigating Controls	Partially
Change Management Procedures	Yes
Business Continuation Planning	Yes
Testing Schedule and Target Production Date	Yes
Sign-off by the Application Owner, Chief Information Officer, and Information Security Management	No

Source: Minnesota Department of Revenue's Security Plan Standard and auditor's review.

Specific to the objectives of this audit, the department had not (as part of the Security Exceptions, Risks, and Mitigating Controls element) formally assessed whether the databases underlying GenTax needed more data protection strategies than required by the Internal Revenue Service. While management asserted that it had considered additional two-factor authentication, full disk and field level encryption, they had not documented the results of their analysis. Without a completed plan, information security staff lacked the guidance necessary to implement and monitor the internal controls to achieve the desired level of protection.

[6] Minnesota Department of Revenue, Security Plan Standard, initial approval September 1, 2000; revised and approved October 26, 2009.

Recommendation

- *The Department of Revenue should complete GenTax's comprehensive security plan in compliance with its standard. In particular, the department should assess system security risks and determine the controls necessary to mitigate those risks.*

Finding 2

The Department of Revenue did not adequately monitor changes to GenTax and its supporting infrastructure to ensure they complied with the department's plan.

The department's internal controls were not effective to adequately mitigate the risk created by allowing certain information technology staff to make changes to GenTax. Although the department logged changes to the system, it had not specified who should review the logs, how the reviewer would validate that the change was authorized, or who to notify if unauthorized or noncompliant changes occurred.

The department's configuration management plan, which documented management's expectations about requesting, testing, and authorizing changes to GenTax,[7] did not clearly address the risk that certain information technology staff could make changes directly to the system. The plan did not address how to detect unauthorized changes or changes that did not comply with management's expectations and was not clear about what types of changes are subject to a documented change control process. The plan required that a formal configuration audit occur for GenTax "prior to any major software release or at the information systems application manager's discretion if the need is determined." A formal configuration audit would test whether employees were complying with authorization and documentation requirements for changes to GenTax. Through November 2012, the department had not performed a formal configuration audit for the GenTax system.

Our testing of changes made to GenTax from July 1, 2011, through September 30, 2012, identified the following instances of noncompliance with the department's configuration management plan:

- The department did not have documentation for 6 of the 25 database changes we tested to show who had authorized the change or whether the change had been tested.

- 1,046 of the 3,756 changes made to GenTax did not include a unique reference number to tie the change back to its supporting request and

[7] Version 1.0, dated June 4, 2012, and approved July 17, 2012.

approval documentation. Starting in April 2012, the department required that all changes would include a reference number as part of the process. However, 200 of the 1,046 changes made after April 2012 did not include a reference number, and 90 of those changes occurred after the department approved the configuration management plan.

Without sufficient controls to prevent or detect unauthorized changes to GenTax, there is an increased risk that a change could negatively impact GenTax's operations and affect the integrity of its underlying data.

Recommendations

- *The Department of Revenue should enhance the GenTax configuration management plan to better specify the applicability of the change control procedures to the types of GenTax changes that can occur.*

- *The Department of Revenue should implement effective monitoring controls to ensure that all changes to GenTax follow its configuration management plan, including reference numbers to link each change to its documentation supporting the authorization and testing of the changes and periodic configuration audits to ensure compliance.*

Finding 3

The Department of Revenue had not clearly documented expectations for its review of reports that tracked changes to or viewing of data within the database or changes to the database structure.

The department did not effectively use reports of changes to or viewing of data by information technology staff in the GenTax databases, or of changes they made to the database structure, to mitigate the risk that it would not detect unauthorized activities. The department had the following weaknesses in its reviews of information technology staff's activities:

- The department had not provided sufficient guidance to staff reviewing daily reports of changes to or viewing of data in the GenTax databases. Without guidance, the staff reviewing the reports may not identify unusual activity or know what to do if they detected it. The department had not documented its expectations about normal trends to better identify activity requiring further review. The department also had not established processes or protocols for documenting and reporting any unusual activity identified.

- The daily report about information technology staff that accessed or modified data directly in the databases did not differentiate between

records that had been changed and those that had been viewed. Because the department's response to an unauthorized data change would likely be different from its response to unauthorized data viewing, not having this information limits the report's effectiveness.

- The department assigned the weekly review of changes to the database structure to database administrators who had access to make those changes and could alter the reports to hide unauthorized changes. Because database administrators were not independent of the transactions being reviewed, the review was not an effective internal control to identify unauthorized changes to the database structure.

Management had not established its expectations about the risks these report reviews were designed to mitigate, how frequently they should be performed, who should perform them, how the reviews should be documented, and how long that documentation should be retained. As a result, unauthorized activity may not be immediately detected.

Recommendation

- *The Department of Revenue should document expectations for reviews designed to detect unauthorized changes to or viewing of data within the database or to the database structure.*

Finding 4

The Department of Revenue had not implemented adequate controls to prevent and detect some inappropriate access to servers and databases supporting GenTax.

The department had not periodically reviewed the appropriateness of access it had granted to employees and contractors to the network and databases supporting GenTax. As of November 2012, the department had not detected and corrected the following unnecessary or undocumented access:

1) Because the department had not reviewed employees' network access each quarter, as required by its policy, it delayed detecting and removing 34 users during the period. For four of these employees, the network access also allowed them inappropriate access to GenTax. The quarterly review had not been performed for over 18 months.

2) None of the 16 information technology employees we tested with access to the database had documented authorization for that access.

3) Five employees with database access had unnecessary database administrator privileges. Four of these employees never needed administrator privileges as part of their job duties, and the fifth employee

no longer needed it. The department lacked a policy that required periodic reviews of employees with database access.

Without sufficient and timely controls to prevent or detect unnecessary access to GenTax's supporting infrastructure, there is an increased risk that the excessive access could negatively impact GenTax's operations and affect the integrity and confidentiality of its underlying data when exploited by authorized or unauthorized users.

Recommendations

- *The Department of Revenue should document rules for access to data and/or require that all authorizations to access infrastructure supporting GenTax are documented.*

- *The Department of Revenue should periodically review the access to infrastructure supporting GenTax to ensure it remains appropriate.*

Finding 5

The Department of Revenue had not finalized its documentation of security configuration baseline standards for infrastructure supporting GenTax.

The department had not finalized the security configuration baselines for the databases and servers that support GenTax. As of November 2012, the security configuration baselines for the databases and servers were in draft. Security configuration baselines define and document the security settings management expects an information system to include or comply with. Security baselines are built on management's assessment of the risks related to configuration settings. Because some components of a system are more critical than others, the baseline security settings for those components may be different than other components. However, when we reviewed the basis for certain configuration settings, department information technology staff were unable to explain how they considered risks in making configuration decisions. Documenting the security baselines helps reduce the risk of security breaches from misconfigured system settings; they also provide the standard to which current system settings can be compared to identify potentially unauthorized changes to the system.

Without a baseline, management cannot identify when current system settings do not align with its expectations. In some cases, the Department of Revenue had documented policies and standards but did not establish methods to ensure that those processes were being followed. Exceptions to processes may result from intentional or unintentional deviations, and good monitoring procedures can inform management on how well controls are designed or areas to improve on.

We tested selected actual configuration settings against some of the department's policies, standards, and settings management told us they believed were in place. We identified some instances where actual settings did not conform to management's expectation. Although the deviations did not present significant security weaknesses, they showed that the department had not established an effective way to identify and correct current system settings that do not align with its expectations.

Recommendations

- *The Department of Revenue should assess the risks associated with the configurations available in the infrastructure supporting GenTax.*

- *The Department of Revenue should complete the security configuration baselines infrastructure supporting GenTax.*

- *The Department of Revenue should periodically compare the system's configuration to its baseline to identify deviations.*

MINNESOTA · REVENUE

February 26, 2013

James Nobles
Legislative Auditor
Room 140 Centennial Building
658 Cedar Street
St. Paul, Minnesota 55155-1603

Dear Mr. Nobles:

Thank you for the work done on the information technology security audit of the Department of Revenue's integrated tax system (GenTax).

We are pleased with your overall conclusion that all systems operated by the Department generally had adequate internal controls to protect tax-related information from unauthorized modification and viewing.

The Department of Revenue recognizes that the security, integrity and proper use of taxpayer information is a fundamental expectation of our taxpayer customers, and essential to the success of our business operations. As such, we have high expectations for data security and proper use of taxpayer information by employees and we will work closely with our MN.IT services team to meet these standards. We appreciate your findings and recommendations for improvement in completing documentation and validating process and procedures.

We have reviewed your recommendations in consultation with MN.IT Services to respond specifically to each recommendation. Those responses are contained on the following pages, and the Department of Revenue will work closely with the MN.IT Services information technology security experts under the leadership of Commissioner Carolyn Parnell to implement these recommendations.

Once again, thank you and your staff for your time and effort on this audit.

Sincerely,

Myron Frans
Commissioner

Recommendation – Finding 1

The Department of Revenue should complete GenTax's comprehensive security plan in compliance with its standard. In particular, the department should assess system security risks and determine the controls necessary to mitigate those risks.

Response:

The Department of Revenue will work with MN.IT Services to finalize the comprehensive security plan in compliance with all applicable standards. A risk assessment for the GenTax Integrated Tax System was performed by Department of Revenue Internal Audit in November-December 2012. Additionally, the IRS conducts a comprehensive safeguard review every three years and requires an annual report on tax information security. Results are being reviewed to determine and document the necessary controls to mitigate identified risks. We anticipate resolution to be completed by June 30, 2013.

Recommendations – Finding 2

The Department of Revenue should enhance the GenTax configuration management plan to better specify the applicability of the change control procedures to the types of GenTax changes that can occur.

The Department of Revenue should implement effective monitoring controls to ensure that all changes to GenTax follow its configuration management plan, including reference numbers to link each change to its documentation supporting the authorization and testing of the changes and periodic configuration audits to ensure compliance.

Response:

The Department of Revenue will work with MN.IT Services staff to review and enhance the configuration management plan to ensure that all system changes follow established change control procedures. Specifically, all changes will be documented and reviewed by appropriate individuals. System changes will also be reviewed to ensure that they conform to established configuration management standards. Finally, periodic reviews will be done to confirm that change and configuration management controls are working as intended. We anticipate resolution to be completed by June 30, 2013.

Recommendation – Finding 3
The Department of Revenue should document expectations for reviews designed to detect unauthorized changes to or viewing of data within the database or to the database structure.

Response:
The Department of Revenue will work to document expectations for reviews to detect unauthorized changes to or viewing of data within the database or to the structure of the database. We anticipate resolution to be completed by September 30, 2013.

Recommendations – Finding 4
The Department of Revenue should document rules for access to data and/or require that all authorizations to access infrastructure supporting GenTax is documented.

The Department of Revenue should periodically review the access to infrastructure supporting GenTax to ensure it remains appropriate.

Response:
Additional policies, procedures and standards, along with clarification of frequency for review are being documented and expanded that will better describe authorization and access to the GenTax Integrated Tax system. The Department of Revenue executive management team has directed Internal Audit to work with MN.IT Services Chief Information Officer at Revenue to ensure regular reviews of access to servers and databases are conducted consistent with documented rules. We anticipate resolution to be completed by December 31, 2013.

Recommendations – Finding 5
The Department of Revenue should assess the risks associated with the configurations available in the infrastructure supporting GenTax.

The Department of Revenue should complete the security configuration baseline infrastructure supporting GenTax.

The Department of Revenue should periodically compare the system's configuration to its baseline to identify deviations.

Response:
The Department of Revenue will work closely with MN.IT Services at Revenue and MN.IT Information Security Manager over Governance, Risk and Compliance to finalize the security configuration baseline infrastructure allowing us to assess risks with configurations baselines

available within the infrastructure. Additionally, periodic review of system configuration against the baseline will be conducted to identify deviation and the ability for correction. We anticipate resolution to be completed by March 1, 2014.