STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-124
February 2019

DEPARTMENT OF REVENUE

System for Unified Taxation (SUNTAX)

Sherrill F. Norman, CPA
Auditor General

Executive Director of the Department of Revenue

The Department of Revenue is established by Section 20.21, Florida Statutes. The head of the Department is the Governor and Cabinet. Pursuant to Section 20.05(1)(g), Florida Statutes, the Governor and Cabinet are responsible for appointing an Executive Director of the Department. Leon M. Biegalski served as Executive Director during the period of our audit.

The team leader was Arthur Wahl, CPA, CISA, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF REVENUE

System for Unified Taxation (SUNTAX)

SUMMARY

This operational audit of the Department of Revenue (Department) focused on evaluating selected information technology (IT) controls applicable to the System for Unified Taxation (SUNTAX) and included a follow-up on the findings included in our report No. 2015-006. Our audit disclosed the following:

Finding 1: Some Department users had inappropriate and unnecessary SUNTAX access privileges. Similar findings were noted in prior audits of the Department.

Finding 2: As similarly noted in prior audits, the Department did not timely deactivate the SUNTAX access privileges of some former employees.

Finding 3: Department procedures for conducting periodic reviews of user access privileges continue to need improvement to ensure the appropriateness of SUNTAX user access privileges.

Finding 4: Certain security controls related to logical access, user authentication, and logging and monitoring continue to need improvement to ensure the confidentiality, integrity, and availability of SUNTAX data and Department IT resources.

BACKGROUND

System for Unified Taxation (SUNTAX) is the Department of Revenue's (Department's) tax administration and accounting system that utilizes a commercial off-the-shelf enterprise resource planning (ERP) software package that uses a common framework across all tax types. SUNTAX provides functions such as:

- One-stop registration to establish a taxpayer's account for all taxes in a single system.
- Processing of all financial tax returns, payments, and related correspondence, including electronic filings.
- Posting of financial transactions to the general ledger and taxpayer account records to maintain accurate accounts receivable and payable across tax types, resulting in accurate distribution of collected funds to the proper taxing authority.
- Maintenance of a taxpayer account including multiple addresses, status for taxes, and a summary of delinquent tax returns and financial obligations.
- Support for the collection of delinquent taxes, identifying new taxpayers, and improving compliance of existing taxpayers.

General Tax Administration (GTA) is the primary user of SUNTAX. GTA is responsible for the administration of tax collection, tax enforcement, tax processing, taxpayer registration, and fund distribution, as well as providing taxpayer assistance and resolving taxpayer complaints. The Department's Information Services Program (ISP) functions include developing, maintaining, and managing systems for tax return processing and taxpayer registration activities, including SUNTAX.

There are four components within SUNTAX:

- ERP Core Component (ECC) – the primary component used to process and store taxpayer master data, returns, payments, and jurisdictional distribution information. It is also used to manage taxpayer accounts receivable and collection process.
- Customer Relationship Management (CRM) – used for business process work activities, refunds review and approvals, and compliance lead development.
- Business Warehouse (BW) – used for reporting and fuel tracking.
- SAP Enterprise Portal – allows internal and external users to view reports and Florida counties to file and pay clerk fees.

FINDINGS AND RECOMMENDATIONS

Finding 1: Appropriateness of Access Privileges

Agency for State Technology (AST) rules[1] require each agency to ensure that access permissions are managed, incorporating the principles of least privilege and separation of duties. Furthermore, effective access controls include a process for the unique identification of system users that allows management to assign responsibility for system activity to an individual and restrict users to only those access privileges necessary for the users' assigned job duties.

Our audit procedures disclosed that some users had inappropriate and unnecessary SUNTAX access privileges. Specifically:

- To determine whether access privileges to maintain business partners (change taxpayer addresses) and access privileges to change billing documents were appropriately restricted to promote an appropriate separation of duties, we evaluated the 145 SUNTAX user accounts assigned both access privileges as of June 20, 2018. Our evaluation disclosed that 25 of the 145 SUNTAX user accounts had been erroneously granted one or both access privileges. Thirteen of the 25 user accounts had been assigned incorrect roles and, for the remaining 12 user accounts, the assigned roles included incorrect access privileges resulting in inappropriate and unnecessary SUNTAX access privileges.
- To determine whether developers were appropriately restricted from having SUNTAX production end-user update access privileges, we evaluated the 34 SUNTAX user accounts assigned developer roles for updating SUNTAX program code or promoting changes to SUNTAX program code as of June 25, 2018. We compared the 34 user accounts to the SUNTAX user access list to determine whether the developer user accounts were also assigned end-user update access roles contrary to an appropriate separation of duties. Our audit procedures disclosed that 32 of the 34 SUNTAX user accounts assigned developer roles were also assigned roles granting SUNTAX production end-user update access privileges, contrary to an appropriate separation of duties.
- To determine whether access privileges to the SUNTAX databases were appropriately restricted we evaluated the 24 SUNTAX user accounts managed by the Department or utilized to back up the databases that were assigned access to one or more of the three SUNTAX databases as of June 14, 2018, and June 26, 2018. Our evaluation of the 24 user accounts disclosed 5 user

[1] AST Rule 74-2.003(1)(d), Florida Administrative Code.

accounts with inappropriate access privileges and 3 user accounts that were shared by multiple users, thereby precluding individual accountability for actions taken.

- To determine whether access privileges to the operating systems of the three servers hosting the SUNTAX databases were appropriately restricted, we evaluated the 45 Department-administered[2] SUNTAX user accounts assigned system-level access to one or more of the three SUNTAX database servers as of June 14, 2018. Our evaluation of the 45 user accounts disclosed 8 user accounts with inappropriate access privileges and 3 user accounts that were shared by multiple users, thereby precluding individual accountability for actions taken.

Our audit procedures also disclosed that the Department did not maintain detailed documentation of the SUNTAX roles that describes the roles and the access privileges provided by the roles. The lack of such documentation impedes management's ability to analyze the significance of the roles assigned and the related access privileges granted to the SUNTAX user accounts and to identify inappropriate and unnecessary SUNTAX access privileges. The existence of inappropriate and unnecessary access privileges increases the risk that unauthorized modification, loss, or disclosure of SUNTAX data and information technology (IT) resources may occur. Additionally, sharing user accounts limits Department management's ability to assign responsibility for system activities. Similar findings were noted in prior audits of the Department, most recently in our report No. 2015-006.

Recommendation: We again recommend that Department management limit user access privileges to SUNTAX to promote an appropriate separation of duties and restrict users to only those access privileges necessary for the users' assigned job duties. We also recommend that Department management ensure that user accounts are individually assigned to promote accountability for actions taken.

Finding 2: Timely Deactivation of Access Privileges

AST rules[3] require agency control measures that ensure IT access is removed when an IT resource is no longer required. Also, the Department's *Information Security Policy*[4] requires access authorization be promptly removed when a user's employment is terminated or access to the information resource is no longer required. Prompt action to deactivate access privileges when a user separates from employment or access to the information is no longer required is necessary to help prevent the misuse of the access privileges.

We compared the list of employees who separated from Department employment during the period July 1, 2017, through June 6, 2018, to the SUNTAX active user accounts as of June 20, 2018, and found that the SUNTAX active user accounts included user accounts for seven former employees. As of June 20, 2018, the seven user accounts had remained active from 32 to 362 days after the users separated from Department employment. In response to our audit inquiry, Department management indicated that, although the user accounts were not timely deactivated, the SUNTAX user access privileges for the seven former employees had not been used subsequent to the respective dates of employment separation.

[2] Accounts administered by AST were not included in our evaluation.

[3] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

[4] Department IT Service Management Policy, Policy Number: IS009, *Information Security Policy*.

Timely deactivation of SUNTAX user accounts upon an employee's separation from Department employment reduces the risk that the SUNTAX access privileges may be misused by the former employee or others. Similar findings were noted in prior audits of the Department, most recently in our report No. 2015-006.

Recommendation: We again recommend that Department management ensure that the SUNTAX user access privileges are timely deactivated upon a user's separation from Department employment.

Finding 3: Periodic Review of User Access Privileges

AST rules[5] require agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. The Department's *Information Security Policy*[6] requires supervisors, through periodic reviews, to ensure employees have the appropriate level of access to Department information resources needed to perform job responsibilities and that the access does not exceed the need. Also, the Department's *Security Risk Analysis Checklist* for SUNTAX stipulates the periodic reviews be performed annually. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. An effective periodic review consists of identifying the current access privileges of all system users and evaluating the assigned access privileges to ensure that they align with the users' job responsibilities.

As part of our audit, we evaluated Department procedures and made inquiries with Department management related to periodic reviews of SUNTAX user access privileges. Our audit procedures disclosed that the Department assessed the risk of users retaining inappropriate access to SUNTAX as low, which resulted in only an annual access review. Based on the criticality of SUNTAX and the inclusion of confidential and sensitive data within the system, and considering the deficiencies described in Findings 1 and 2, an annual access review appears insufficient. Additionally, we noted that the last three reviews of SUNTAX user access privileges, completed in August 2016, August 2017, and December 2018, were not comprehensive. Specifically, the reviews included only the SUNTAX access privileges for GTA users and did not include Department support staff, such as ISP users.

The performance of an effective and comprehensive review of all SUNTAX user access privileges biannually or quarterly would increase management's assurance that the access privileges assigned to SUNTAX users remain appropriate. Similar findings were noted in prior audits of the Department, most recently in our report No. 2015-006.

Recommendation: We again recommend that Department management perform comprehensive and effective periodic reviews of SUNTAX user access privileges to verify that the access privileges remain appropriate. Department management should reassess the frequency of the periodic reviews of SUNTAX user access privileges to better align with the criticality of the system and the confidential and sensitive data therein.

[5] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

[6] Department IT Service Management Policy Number IS009, *Information Security Policy.*

Finding 4: Security Controls – Logical Access, User Authentication, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed certain security controls related to logical access, user authentication, and logging and monitoring for SUNTAX and related IT resources continue to need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising SUNTAX data and IT resources. However, we have notified appropriate Department management of the specific issues.

Without adequate security controls related to logical access, user authentication, and logging and monitoring controls for SUNTAX and related IT resources, the risk is increased that the confidentiality, integrity, and availability of SUNTAX data and related IT resources may be compromised. Similar findings were communicated to Department management, most recently in connection with our report No. 2015-006.

Recommendation: We recommend that Department management improve certain security controls related to logical access, user authentication, and logging and monitoring for SUNTAX and related IT resources to ensure the continued confidentiality, integrity, and availability of SUNTAX data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2015-006.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from May 2018 through October 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected application-level general controls applicable to SUNTAX during the period July 2017 through September 2018, and selected actions prior and subsequent thereto. The overall objectives of the audit were:

- To evaluate the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.

- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2015-006.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Department personnel and reviewed Department documentation to obtain an understanding of:
  - SUNTAX background information and business process flows including key sources of data input, application transactions and processes, and types of application data output, including interfaces.
  - The SUNTAX computing platform, including applicable hardware, operating system, database management system, and security software.
- Evaluated the logical design, appropriateness, administration procedures and related documentation for SUNTAX. Specifically, we:
  - Evaluated the 145 SUNTAX user accounts assigned access privileges to maintain business partners (change taxpayer addresses) and to change billing documents as of June 20, 2018, to determine whether the user accounts were necessary and appropriately restricted to promote an appropriate separation of duties.

- Evaluated the 34 SUNTAX user accounts assigned developer roles for updating SUNTAX program code or promoting changes to SUNTAX program code through the change management process to determine whether the developers were restricted from having SUNTAX production end-user update access privileges.
- Compared the list of employees who separated from Department employment during the period July 1, 2017, through June 6, 2018, to the active user accounts defined in SUNTAX as of June 20, 2018, to determine whether any former employees had active SUNTAX access privileges. For the seven former employees we identified with an active SUNTAX user account as of June 20, 2018, we determined whether the access privileges were used subsequent to the employment separation dates.
- Evaluated the appropriateness of access as of June 20, 2018, and June 26, 2018, for 135 of the 142 user accounts assigned one or more of three high-risk SUNTAX transaction codes.
- Evaluated the adequacy of the 2016, 2017, and 2018 annual reviews of SUNTAX user access privileges.

- Evaluated selected SUNTAX application change management controls. Specifically, we evaluated:
  - Department procedures for application change management related to SUNTAX to assess whether the procedures were designed to reasonably assure that SUNTAX program changes were documented, authorized, and tested.
  - The effectiveness of change management controls for 30 of the 307 completed SUNTAX application program change requests implemented from July 1, 2017, through June 5, 2018, to determine whether program change requests were appropriately documented, authorized, tested, approved for production, and moved into production by authorized personnel separate from the developer.
- Evaluated the logging and monitoring controls related to the SUNTAX application to determine whether the use of sensitive transactions and changes to production tables are logged and monitored and whether security events such as assignments to high-level profiles, security assignment changes, and system profile parameter setting changes are logged and monitored.
- Evaluated the SUNTAX interface procedures related to the Imaging Management System to assess whether the procedures were designed to reasonably assure that the interfaces were processed accurately, completely, and timely, and rejected interface data was isolated, analyzed, and corrected timely.
- Evaluated selected controls to protect sensitive SUNTAX resources. Specifically, we evaluated:
  - The 24 SUNTAX user accounts managed by the Department or utilized to back up the databases assigned access to one or more of the three SUNTAX databases as of June 14, 2018, and June 26, 2018, to determine whether access privileges were appropriately restricted.
  - The 45 Department-administered SUNTAX user accounts assigned system-level access to one or more of the three SUNTAX database servers as of June 14, 2018, to determine whether access privileges to the operating systems of the three servers hosting the SUNTAX databases were appropriately restricted.
- Evaluated logging and monitoring controls related to the use of sensitive or privileged accounts that directly access the SUNTAX database.
- Evaluated the appropriateness of authentication and identification controls for the four components of SUNTAX and for the SUNTAX external file transfer server as of June 21, 2018, July 18, 2018, and the network inactivity limit setting as of October 16, 2018.

- Evaluated selected remote access security configurations for transmitting SUNTAX data containing confidential and sensitive information.
- Evaluated Department policy and procedures for strategic risk management and reviewed the SUNTAX risk assessment to ensure that the Department periodically reviews the SUNTAX application security and maintains an up-to-date SUNTAX risk assessment.
- Reviewed the SUNTAX Disaster Recovery Plan and related documentation and evaluated whether sufficient documentation for recoverability was maintained, a live test of the plan was conducted annually, documentation of test results was maintained, and test result action items were resolved.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

Florida Department of Revenue
Office of the Executive Director

Jim Zingale
Executive Director

5050 West Tennessee Street, Tallahassee, FL 32399

floridarevenue.com

February 8, 2019

Ms. Sherrill F. Norman, CPA
Auditor General
Office of the Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

As required by section 11.45(4)(d), Florida Statutes, attached is the Department's response to the preliminary and tentative findings and recommendations included in your report for the audit of the Department of Revenue System for Unified Taxation (SUNTAX).

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact Marie Walker, Director of Auditing, at 717-7598 or Marie.Walker@floridarevenue.com.

Sincerely,

Jim Zingale

JZ/mw

Attachment

cc: Brenda Shiner, Audit Manager
Art Wahl, Audit Team Leader
Andrea Moreland, Deputy Executive Director
Maria Johnson, General Tax Administration Program Director
Damu Kuttikrishnan, Information Services Program Director
Sharon Doredant, Inspector General
Marie Walker, Director of Auditing

Department of Revenue
Auditor General SUNTAX Audit
Preliminary and Tentative Response

Finding 1: Some Department users had inappropriate and unnecessary SUNTAX access privileges. Similar findings were noted in prior audits of the Department.

Recommendation: We again recommend that Department management limit user access privileges to SUNTAX to promote an appropriate separation of duties and restrict users to only those access privileges necessary for the users' assigned job duties. We also recommend that Department management ensure that user accounts are individually assigned to promote accountability for actions taken.

Response: We agree with the finding and recommendations. We will identify user accounts that have inappropriate levels of access to SUNTAX databases and server operating systems and restrict them. We will ensure that duties with update access are separated between SUNTAX development and production environments, and between users with access to update taxpayers addresses and billing documents. SUNTAX accounts will be reviewed to ensure there is no sharing among multiple users. The roles will have their descriptions and access privileges documented to assist the process to review appropriateness.

Finding 2: As similarly noted in prior audits, the Department did not timely deactivate the SUNTAX access privileges of some former employees.

Recommendation: We again recommend that Department management ensure that the SUNTAX user access privileges are timely deactivated upon a user's separation from Department employment.

Response: We agree with the finding and recommendations. An extra verification step will be added to the account deactivation process to ensure user access is removed in a timely manner after every separation from the Department and when a user transfers internally to another position that does not require SUNTAX access.

Finding 3: Department procedures for conducting periodic reviews of user access privileges continue to need improvement to ensure the appropriateness of SUNTAX user access privileges.

Recommendation: We again recommend that Department management perform comprehensive and effective periodic reviews of SUNTAX user access privileges to verify that the access privileges remain appropriate. Department management should reassess the frequency of the periodic reviews of SUNTAX user access privileges to better align with the criticality of the system and the confidential and sensitive data therein.

Response: We agree with the finding and recommendation. We currently conduct annual reviews of SUNTAX user access privileges. We will need to assess this process and ensure that it meets our needs and is aligned with the criticality of the system.

Finding 4: Certain security controls related to logical access, user authentication, and logging and monitoring continue to need improvement to ensure the confidentiality, integrity, and availability of SUNTAX data and Department IT resources.

Recommendation: We recommend that Department management improve certain security controls related to logical access, user authentication, and logging and monitoring for SUNTAX and related IT resources to ensure the continued confidentiality, integrity, and availability of SUNTAX data and related IT resources.

Response: We agree with the finding and recommendations. ISP will work with the General Tax Administration business process to implement improvements and increase security controls.