Office of the Auditor General

Performance Audit Report

Michigan Integrated Tax Administration System

Department of Treasury and
Department of Technology, Management, and Budget

March 2020

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

271-0595-19

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

The auditor general may make investigations pertinent to the conduct of audits.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit

Michigan Integrated Tax Administration System (MIITAS)

Department of Treasury (Treasury) and Department of Technology, Management, and Budget (DTMB)

Report Number:
271-0595-19

Released:
March 2020

MIITAS is used to administer various State business and City of Detroit taxes, such as the Michigan Business Tax; Corporate Income Tax; sales, use, and withholding taxes; and City of Detroit individual income tax. MIITAS is an SAP solution that was implemented by Treasury and DTMB in 2008. Since 2007, Treasury and DTMB have contracted with three vendors for the development, enhancement, and maintenance of MIITAS, cloud hosting, software licensing, and training and consulting for a total cost of $129.0 million. In fiscal year 2018, Treasury processed approximately $19.7 billion in tax revenues and $1.0 billion in tax refunds through MIITAS.

Audit Objective			**Conclusion**
Objective #1: To assess the effectiveness of selected security and access controls over MIITAS.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Security-related events, such as changes to sensitive and confidential information, were not monitored for appropriateness (Finding #1).	X		Agrees
High-risk access within MIITAS was not sufficiently restricted. We noted that 10 (14%) transaction codes and 22 (69%) authorization objects assigned to users were not appropriate for the users' job responsibilities (Finding #2).	X		Agrees
Security configuration checklists and baseline configurations were not developed for MIITAS to ensure protection from threats and vulnerabilities (Finding #3).		X	Agrees
Vulnerability management improvements were needed because 44% of vulnerabilities from vendor security advisories had not been remediated and the remaining 56% of vulnerabilities were not remediated in the required time frame (Finding #4).		X	Agrees

Audit Objective			Conclusion
Objective #2: To assess the sufficiency of selected tax processing controls within MIITAS.			Sufficient
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Improvements are needed to interface controls because 113 tax refund payments, totaling $7.3 million, were not sent to the address provided by the taxpayer on the tax return (Finding #5).		X	Agrees

Audit Objective			Conclusion
Objective #3: To assess the effectiveness of Treasury and DTMB's change controls over MIITAS.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Sufficient testing was not performed of MIITAS changes. Testing plans were not developed and positive test results were not maintained for 100% of the system changes reviewed (Finding #6).		X	Agrees

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

OAG

Office of the Auditor General

Doug A. Ringler, CPA, CIA
Auditor General

201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • audgen.michigan.gov

March 20, 2020

Ms. Rachael Eubanks
State Treasurer
Richard H. Austin Building
Lansing, Michigan
and
Ms. Tricia L. Foster, Director
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Ms. Eubanks and Ms. Foster:

This is our performance audit report on the Michigan Integrated Tax Administration System (MIITAS), Department of Treasury and Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agencies provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

MICHIGAN INTEGRATED TAX ADMINISTRATION SYSTEM

Page

Report Summary 1

Report Letter 3

Audit Objectives, Conclusions, Findings, and Observations

Selected Security and Access Controls 8

Findings:

1. Monitoring of security-related events needed. 9
2. Effective access controls not established and implemented. 11
3. Improvements needed over configuration management controls. 15
4. Vulnerability management process improvements needed. 17

Selected Tax Processing Controls 19

Findings:

5. Improvements needed in tax refund interface controls. 21

Change Controls 22

Findings:

6. Change management process improvements needed. 23

System Description 25

Audit Scope, Methodology, and Other Information 26

Glossary of Abbreviations and Terms 30

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

SELECTED SECURITY AND ACCESS CONTROLS

BACKGROUND

Security controls are the management, operational, and technical controls designed to protect the availability*, confidentiality*, and integrity* of a system and its information.

Access controls* limit or detect inappropriate access to computer resources, thereby protecting the resources from unauthorized modification, loss, and disclosure. For access controls to be effective, they should be properly authorized, implemented, and maintained.

State employees and contractors access the Michigan Integrated Tax Administration System (MIITAS) through the SAP Enterprise Portal or SAPGUI*. As of July 2019, approximately 800 State employees and contractors from the Department of Treasury (Treasury), the Department of Technology, Management, and Budget (DTMB), and other agencies had access to MIITAS.

AUDIT OBJECTIVE

To assess the effectiveness* of selected security and access controls over MIITAS.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- All system components that we reviewed were supported by the vendor, and some security configuration parameters were implemented in accordance with State standards and industry best practices.

- Vulnerability scans were conducted for 90% of the MIITAS servers, and controls were implemented to remediate some vulnerabilities*.

- Some access controls were implemented in accordance with State policies and standards.

- Two material conditions* related to monitoring security-related events and establishing and implementing effective access controls (Findings #1 and #2).

- Two reportable conditions* related to establishing and implementing effective configuration management controls and improving the vulnerability management process (Findings #3 and #4).

** See glossary at end of report for definition.*

FINDING #1

Monitoring of security-related events needed.

Treasury, in conjunction with DTMB, did not monitor security-related events within MIITAS to help facilitate the ongoing awareness of threats*, vulnerabilities, and information security*.

Information systems that contain critical data, such as tax information, require monitoring countermeasures across a broad range of areas to adequately protect the data from threats.

State of Michigan (SOM) Technical Standard 1340.00.040.01 requires that Treasury and DTMB determine the events to be monitored based on current threat information and ongoing risk assessments. Treasury policy ET-03168 requires that audit logs be periodically reviewed for security-related events. Examples of events not reviewed include:

Changes to sensitive and confidential information were not monitored.

- Addition, modification, deletion, or viewing of sensitive and confidential information.
- Suspected fraudulent transactions.
- Privileged user activities.
- Changes to security privileges.
- Activities that violate established security standards or configurations.
- Unauthorized access attempts.
- Use of elevated access rights.

Treasury and DTMB informed us that they monitor tax refunds with an address change on a daily basis to mitigate fraud risk; however, they did not implement logging and monitoring processes for other security-related events.

This finding represents a material condition because, without effective monitoring, Treasury and DTMB cannot ensure the appropriateness of privileged activities and system changes or the timely identification of other unauthorized activities.

RECOMMENDATION

We recommend that Treasury, in conjunction with DTMB, monitor security-related events within MIITAS to help facilitate the ongoing awareness of threats, vulnerabilities, and information security.

AGENCY PRELIMINARY RESPONSE

Treasury and DTMB provided us with the following response:

Treasury and DTMB agree with the recommendation. Treasury and DTMB were aware of this weakness and initiated a project in 2018 to select and implement a Governance, Risk and Compliance (GRC) tool. The GRC tool was successfully

** See glossary at end of report for definition.*

implemented and deployed in September 2019 and, along with the improved business processes, provides the capability to monitor security-related events within MIITAS. Treasury and DTMB continue to develop and implement procedures to facilitate the ongoing awareness of threats, vulnerabilities, and information security.

FINDING #2

Effective access controls not established and implemented.

Treasury did not fully establish and implement effective access controls over MIITAS to help ensure that data is secure and system controls are operating as intended.

SOM Technical Standard 1340.00.020.01 defines the security control baselines for access to information systems. The Standard requires that access be managed and periodically reviewed to ensure that access is based on the principle of least privilege*. Access to MIITAS is enabled through SAP functionality where transaction codes* and authorization objects* are granted to users through roles and profiles that control user activity.

Our review disclosed:

a. Treasury did not sufficiently restrict high-risk access within MIITAS in accordance with Treasury policy ET-03179. We noted:

(1) For 73 judgmentally sampled high-risk transaction codes:

(a) 10 (14%) transaction codes assigned to users were not appropriate for the users' job responsibilities. We determined that 92 users had access to these transaction codes.

(b) 17 (23%) transaction codes should be locked and not regularly accessible. We noted that 113 users had inappropriate access to these transaction codes.

Examples of high-risk transaction codes include program execution, table maintenance, and user account administration.

(2) For 32 judgmentally sampled high-risk authorization objects:

(a) 22 (69%) authorization objects assigned to users were not appropriate for the users' job responsibilities. We determined that 467 users had access to these authorization objects.

(b) 8 (25%) authorization objects should be further restricted to limit the risk posed to MIITAS. We noted that 723 users had access to these authorization objects.

Examples of high-risk authorization objects include table edits, releasing system code, and job scheduling.

69% of reviewed high-risk authorization objects assigned to users were not appropriate for the users' job responsibilities.

** See glossary at end of report for definition.*

(3) For 6 (10%) of 58 judgmentally sampled instances of elevated access rights assigned to users:

(a) 3 (50%) access requests did not contain sufficient justification for use of the elevated access rights.

(b) 3 (50%) access requests to assign the elevated access rights did not have the approval documented.

(c) 2 (33%) assignments of elevated access rights were not revoked in a timely manner.

The elevated access rights allow unlimited access to MIITAS, including functional tax areas and security administration.

b. Treasury did not fully implement effective controls over non-user accounts.

SOM Technical Standard 1340.00.020.01 requires that non-user accounts, such as system, service, and generic accounts, be assigned to an account manager and be restricted to necessary access rights. Also, MIITAS contains default user accounts that should be locked and regularly reviewed to ensure protection of MIITAS.

Specifically:

(1) We judgmentally and randomly sampled 4 (12%) of 33 system accounts and noted:

(a) 2 (50%) accounts had excessive access rights.

(b) 1 (25%) account was not locked as recommended by best practices.

(c) 1 (25%) account was not assigned an account manager.

(2) We noted that 6 (35%) of 17 default user accounts were not locked as recommended by best practices.

c. Treasury should improve its periodic access review process.

Treasury policy ET-03164 requires annual reviews to ensure the appropriateness of user access rights in accordance with job responsibilities. The policy also requires that users who no longer need MIITAS access be removed within 48 hours.

We randomly and judgmentally sampled 4 (17%) of 23 divisions within Treasury and DTMB to assess the May 2019 review process results. We noted that 12 (52%) of 23 user accounts were not removed in a timely manner, with each account deletion occurring 23 days after the request.

d. Treasury should improve its segregation of duties* over incompatible job functions.

   Treasury policy ET-03173 requires that the segregation be implemented to reduce risks such as incorrect transaction processing and implementation of improper program changes.

   Treasury's segregation is managed through designed roles by business function. However, implementation of a segregation matrix along with automated tools to prevent and detect violations would help ensure that access is appropriately segregated to reduce security risks.

e. Treasury should improve its documentation of user access.

   Treasury policy ET-03164 requires approval of appropriate user access requests. We randomly and judgmentally sampled 52 users and reviewed the 105 corresponding access requests. We noted:

   (1) 31 (30%) access requests did not contain adequate information to support the access being requested. However, the access granted to each user was appropriate.

   (2) 13 (12%) access requests did not contain the required approval signatures.

Treasury informed us that further evaluation was needed of high-risk access and that reliance on manual controls contributed to the deficiencies noted.

This finding represents a material condition because of the importance of user access in securing MIITAS, the sensitive nature of MIITAS, and the collective number of deficiencies identified.

RECOMMENDATION

We recommend that Treasury fully establish and implement effective access controls over MIITAS to help ensure that data is secure and system controls are operating as intended.

** See glossary at end of report for definition.*

AGENCY PRELIMINARY RESPONSE

Treasury provided us with the following response:

Treasury agrees with the recommendation. Treasury was aware of weaknesses with access control processes and initiated a project in 2018 to select and implement a Governance, Risk and Compliance (GRC) tool. The GRC tool was successfully implemented and deployed in September 2019 and along with the improved business processes, have mitigated and reduced these weaknesses. Treasury continues to refine its use of the GRC tool to enforce least privileged access and to better monitor access within the system.

FINDING #3

Improvements needed over configuration management controls.

DTMB, in conjunction with Treasury, did not fully establish and implement effective configuration management controls to ensure that MIITAS is protected from threats and vulnerabilities.

According to the National Institute of Standards and Technology* (NIST), organizations can control vulnerabilities and reduce threats by implementing a robust security configuration management process. Configuration management controls help ensure the availability, confidentiality, and integrity of information systems.

Specifically, DTMB, in conjunction with Treasury, did not:

a. Formally develop security configuration checklists* and baseline configurations* for MIITAS.

   SOM Technical Standard 1340.00.060.01 requires that configuration settings be established and documented within security configuration checklists that reflect the most restrictive mode consistent with operational requirements. The Standard also requires that baseline configurations be developed, documented, and maintained to reflect the current enterprise architecture.

   DTMB and Treasury informally use vendor guidance and State policy as the basis for MIITAS security configurations.

b. Establish a process to monitor and review MIITAS security configurations.

   SOM Technical Standard 1340.00.060.01 requires that changes to configuration settings be monitored and controlled in accordance with organizational policies and procedures. According to NIST Special Publication 800-128, organizations should perform security-focused configuration management monitoring, including:

   - Querying audit records or logs to monitor and identify unauthorized change events.

   - Running system integrity checks to verify that configurations have not been changed.

   - Reviewing change control* records to verify conformance with configuration management policy.

c. Conduct security impact analyses and document and approve deviations from security configuration checklists and baseline configurations.

** See glossary at end of report for definition.*

SOM Technical Standard 1340.00.060.01 requires that any deviations from secure configurations be identified, documented, and approved. The Standard also requires that configuration changes be analyzed to determine potential security impacts prior to change implementation.

d. Fully configure MIITAS in accordance with SOM standards and industry best practices.

   We reviewed selected security configuration parameters and identified deviations from SOM standards and industry best practices. Because of the confidentiality of these configurations, we summarized our testing results for presentation in this finding and provided the underlying details to DTMB and Treasury management.

RECOMMENDATION

We recommend that DTMB, in conjunction with Treasury, fully establish and implement effective configuration management controls to ensure that MIITAS is protected from threats and vulnerabilities.

AGENCY PRELIMINARY RESPONSE

DTMB and Treasury provided us with the following response:

DTMB and Treasury agree with the recommendation. DTMB identified gaps in the configuration management process and addressed these gaps. In January 2020, DTMB completed implementation of new configuration management tools. DTMB continues to develop documentation and procedures to fully establish effective configuration management controls. These activities will be completed by September 30, 2020.

FINDING #4

Vulnerability management process improvements needed.

DTMB should improve its MIITAS vulnerability management process to ensure that threats are identified and remediated to reduce the risk of exploitation.

According to NIST, organizations should implement a vulnerability management program to help reduce or eliminate the potential for exploitation of threats. NIST states that timely remediation of vulnerabilities is critical to maintaining the operational availability, confidentiality, and integrity of information systems.

Our review of DTMB's vulnerability management process disclosed that DTMB did not:

a. Timely evaluate and remediate all vulnerabilities identified by vendor security advisories.

   SAP issues Security Notes that explain known vulnerabilities that exist within SAP software. The Security Notes contain information on the severity of the vulnerabilities, system components impacted, and expert advice on how to mitigate the vulnerabilities.

   SOM Technical Standard 1340.00.150.01 requires that DTMB identify security patches and vulnerabilities from vendor security advisories. The Standard outlines the time frame in which DTMB should complete the remediation of identified vulnerabilities.

   We randomly and judgmentally sampled 18 SAP Security Notes and corresponding vulnerabilities to evaluate the relevancy to MIITAS. Our review of the 9 relevant vulnerabilities disclosed:

   (1) 4 (44%) vulnerabilities classified as medium severity had not been remediated.

   (2) 5 (56%) vulnerabilities classified as critical or medium severity were not remediated in the required time frame.

   DTMB informed us that, prior to its recently implemented SAP Security Note management process, only critical severity notes were regularly reviewed.

b. Fully implement an effective vulnerability scanning process for all MIITAS servers.

   SOM Technical Standard 1340.00.150.01 requires that vulnerability scans be performed every 30 days on all servers supporting an information system. The Standard outlines the time frame in which the remediation of identified vulnerabilities should be completed.

Our review of scan and vulnerability histories disclosed that DTMB did not:

(1) Conduct vulnerability scans for 4 (10%) of 41 servers supporting MIITAS.

(2) Timely remediate all vulnerabilities identified by vulnerability scans.

We identified vulnerabilities that were not remediated within the required time frame as well as vulnerabilities that existed on the servers.

DTMB informed us that, because of issues with its cloud service provider, it did not patch MIITAS servers for a period of time, which contributed to the vulnerabilities identified.

RECOMMENDATION

We recommend that DTMB improve its MIITAS vulnerability management process to ensure that threats are identified and remediated to reduce the risk of exploitation.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and continues to improve its vulnerability management for MIITAS. In March 2020, DTMB will implement a monthly cadence of patching to ensure timeliness of security patches.

SELECTED TAX PROCESSING CONTROLS

BACKGROUND

MIITAS performs administration of various State business and City of Detroit taxes using SAP software. These processes include:

- Loading of tax return and payment information from external sources.
- Processing of tax returns according to specified business rules of each tax and form type.
- Determination and issuance of tax refunds.
- Matching of tax liabilities with payments and identification of accounts for debt collection.

Interface controls* ensure the accurate, complete, and timely processing of data between systems. MIITAS has more than 50 outbound and inbound interfaces, such as:

- Internal Revenue Service (IRS): Electronically filed tax returns are sent to MIITAS.
- JPMorgan Chase (JPMC): Paper tax returns and payments sent to the State's bank are imaged and loaded into MIITAS.
- Michigan Taxpayers Online (MTO): Taxpayers or their agents log on to MTO and upload tax returns or payments, which are sent to MIITAS.
- Statewide Integrated Governmental Management Applications* (SIGMA): Tax refund payments are sent from MIITAS to the State's accounting system for payment.
- State Treasury Accounts Receivable System (STAR): Outstanding tax liabilities are sent to the State's collection system from MIITAS.

AUDIT OBJECTIVE

To assess the sufficiency of selected tax processing controls within MIITAS.

CONCLUSION

Sufficient.

** See glossary at end of report for definition.*

FACTORS IMPACTING CONCLUSION

- 100% of tax processing rules reviewed functioned in accordance with system specifications.

- We validated the reconciliations performed by Treasury and DTMB of interfaced data for 91% of interfaces reviewed.

- Tax processing data reviewed was generally complete and accurate.

- Interface design documentation and reconciliation procedures generally complied with industry best practices for 91% of interfaces reviewed.

- One reportable condition related to improving tax refund interface controls (Finding #5).

FINDING #5

Improvements needed in tax refund interface controls.

Treasury should improve its interface controls to ensure that tax refund checks are sent to the taxpayer address indicated on the return.

MIITAS simultaneously interfaces tax refund payments and taxpayer address modifications to SIGMA to ensure that refund checks are sent to the address on each taxpayer's return. If the address modification interface fails, the refund payment will still be processed and sent to a default payment address on the taxpayer's account in SIGMA. Although the SIGMA address is associated with the taxpayer, it may not be current or may not be associated with the specific business tax return filed.

The Federal Information System Controls Audit Manual* (FISCAM) states that interface controls should be established and implemented to reasonably ensure that data transferred from a source system to a receiving system is processed accurately, completely, and timely.

We reviewed 4,233 interfaced tax refund payments, totaling $141.3 million, from June 1, 2018 through June 30, 2019 and compared the address from the return with the address associated with the refund check issued in SIGMA. Our review disclosed that 113 (3%) refund payments, totaling $7.3 million (5%), were not sent to the address provided by the taxpayer on the return.

Treasury informed us that it corrects and reprocesses failed address modification interface records to help ensure that future tax refund payments are sent to the address on the return; however, Treasury does not review or follow up on payments not sent to the return address for appropriateness. Treasury also informed us that interfaced vendor modification records sometimes fail because of incorrect syntax in the interface file coming from MIITAS.

RECOMMENDATION

We recommend that Treasury improve its interface controls to ensure that tax refund checks are sent to the taxpayer address indicated on the return.

AGENCY PRELIMINARY RESPONSE

Treasury provided us with the following response:

Treasury agrees with the recommendation. Undeliverable refunds are returned to Treasury to be reviewed and processed.

In January 2020, processes were implemented to allow address updates prior to sending the refund.

* *See glossary at end of report for definition.*

CHANGE CONTROLS

BACKGROUND

Changes to MIITAS are typically initiated when Treasury authorizes a needed modification. DTMB or a third-party vendor then constructs the change in a development environment before moving to a test environment. While in the test environment, a change undergoes various quality assurance and user acceptance testing. Upon completion of testing, Treasury authorizes DTMB to move the change into the production environment. After production implementation, Treasury conducts a postimplementation review to verify that the change met user expectations.

MIITAS changes generally consist of new system development projects, break-fixes, and minor system enhancements. Examples of needed modifications include statutory tax changes, system upgrades, remediation of audit findings, and corrections to system functionality.

AUDIT OBJECTIVE

To assess the effectiveness of Treasury and DTMB's change controls over MIITAS.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- 100% of system development projects reviewed were implemented in accordance with State policies, standards, and procedures.

- Some controls were implemented for system changes, including break-fixes and minor system enhancements, in accordance with State policies, standards, and procedures.

- One reportable condition related to implementing effective change controls (Finding #6).

FINDING #6

Change management process improvements needed.

Treasury, in conjunction with DTMB, did not fully implement effective change controls over MIITAS to ensure that system changes are authorized and operating as intended before implementation.

SOM policy 1355.00 establishes project management best practices as a component of the State Unified Information Technology Environment* (SUITE). SOM Technical Procedure 1340.00.060.04.01 establishes the standard methods required for change management.

We randomly sampled 12 (10%) of 119 MIITAS changes, including break-fixes and minor system enhancements, made from June 2018 through May 2019. Our review of Treasury and DTMB's change controls disclosed:

a. Treasury and DTMB did not perform sufficient testing of MIITAS changes.

   SOM Technical Procedure 1340.00.060.04.01 requires development, quality assurance, and user acceptance testing to be performed for all system changes. The Technical Procedure also requires that testing plans be developed and test results be maintained. Specifically, we noted:

   (1) Testing plans were not developed for any of the 12 (100%) system changes reviewed.

       According to FISCAM, detailed testing plans should be developed that define the levels and types of tests necessary for system changes and the testing plans should be documented and approved by all responsible parties. SOM Technical Procedure 1340.00.060.04.01 outlines the standard testing plans required.

   (2) Detailed positive test results were not maintained for any of the 12 (100%) system changes reviewed.

       FISCAM states that test results should be documented and approved before implementation of the corresponding system change. SOM Technical Procedure 1340.00.060.04.01 outlines the required testing results and error tracking for system changes.

   (3) Appropriate segregation of duties was not implemented over all levels of testing.

* *See glossary at end of report for definition.*

SOM Technical Procedure 1340.00.060.04.01 requires segregation of duties for change management. Specifically, quality assurance testing should be performed by DTMB and user acceptance testing should be performed by Treasury.

MIITAS quality assurance and user acceptance testing were performed simultaneously by Treasury. Because quality assurance testing is technical in nature, it should be performed by DTMB to help prevent and detect errors or irregularities in testing and help ensure that system changes are appropriate.

b. DTMB did not perform structured walkthroughs for any of the 12 (100%) system changes reviewed.

   SOM Technical Procedure 1340.00.060.04.01 requires structured walkthroughs for changes and defines the requirements. According to SUITE, structured walkthroughs should be used to identify and correct errors early in the development process to reduce the time and costs resulting from potential rework.

c. Treasury did not perform postimplementation approval for 6 (50%) of the 12 system changes reviewed.

   SOM Technical Procedure 1340.00.060.04.01 requires that the business owner perform postimplementation validation of system changes to ensure that they were applied and function as intended.

RECOMMENDATION

We recommend that Treasury, in conjunction with DTMB, fully implement effective change controls over MIITAS to ensure that system changes are authorized and operating as intended before implementation.

AGENCY PRELIMINARY RESPONSE

Treasury and DTMB provided us with the following response:

Treasury and DTMB agree with the recommendation. In June 2019, test plans were fully implemented for maintenance and operations change activity. A Technical Review Board was convened to perform structured walkthroughs.

Beginning in January 2020, DTMB implemented full separation of duties for maintenance and operations activities by executing System Integration Testing (SIT) in advance of Treasury User Acceptance Testing (UAT). Positive and negative test result evidence have been maintained since January 2020.

SYSTEM DESCRIPTION

MIITAS was implemented by Treasury and DTMB in 2008 to administer the new Michigan Business Tax (MBT). Since then, the following taxes have been added to MIITAS:

- Corporate Income Tax.
- Flow-Through Withholding.
- Sales, use, and withholding taxes.
- City of Detroit individual income, withholding, and corporate taxes.
- Essential Services Assessment.
- Medical Marijuana Facilities tax.

The SAP ECC software, using the Tax and Revenue Management solution, provides the core tax processing functionality of MIITAS. Approximately 800 State employees and contractors access MIITAS via the SAP Enterprise Portal or SAPGUI. Over 300,000 taxpayers also access MIITAS using MTO, a custom Web application. MIITAS has more than 50 interfaces, including the IRS, JPMC, and SIGMA. Since 2007, Treasury and DTMB contracted with three vendors for the development, enhancement, and maintenance of MIITAS, cloud hosting, software licensing, and training and consulting for a total cost of $129.0 million. In fiscal year 2018, Treasury processed approximately $19.7 billion in tax revenues and $1.0 billion in tax refunds through MIITAS.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine MIITAS and other records related to selected security and access, selected tax processing, and change controls of MIITAS. We conducted this performance audit* 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit did not include assessing the City of Detroit's controls over its individual income, withholding, and corporate taxes.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered June 1, 2018 through September 30, 2019.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of MIITAS in order to establish our audit objectives, scope, and methodology. During our preliminary survey, we:

- Obtained an understanding of MIITAS and the various components that make up MIITAS.

- Reviewed applicable policies, standards, procedures, and other best practices for State and SAP information systems.

- Interviewed management and staff responsible for administering and securing MIITAS.

- Reviewed the contract with the MIITAS hosting vendor and assessed corresponding security control reports.

- Surveyed the 780 MIITAS users and evaluated the 398 responses received to further our understanding of user access, tax processing controls, known and potential system issues, and overall user knowledge and satisfaction with MIITAS.

OBJECTIVE #1

To assess the effectiveness of selected security and access controls over MIITAS.

** See glossary at end of report for definition.*

To accomplish this objective, we:

- Evaluated DTMB and Treasury's configuration management controls and reviewed selected security configuration parameters as of June 12, 2019 for the SAP ECC production client and SAP Enterprise Portal for compliance with State standards and industry best practices.

- Reviewed selected MIITAS components as of June 5, 2019 to validate that each component was supported by the vendor.

- Randomly and judgmentally sampled 18 of 171 SAP Security Notes as of June 10, 2019 and evaluated the corresponding vulnerabilities for relevancy to MIITAS. We assessed DTMB's remediation efforts for compliance with State standards for the 9 vulnerabilities determined to be relevant.

- Reviewed scan and vulnerability history reports, generally covering August 2018 through July 2019, of the servers supporting MIITAS to validate that the scans were completed and the corresponding vulnerabilities identified were remediated in accordance with State standards.

- Evaluated the appropriateness of the users assigned access to a judgmental sample of 32 of 3,768 authorization objects as of August 29, 2019 and a judgmental sample of 73 of 143,202 transaction codes as of September 16, 2019.

- Evaluated the design of Treasury's segregation of duties access controls.

- Randomly and judgmentally selected 52 of 767 users as of July 23, 2019 and evaluated the:

    - Appropriateness of the users' access.

    - Users' employment status.

    - Sufficiency of the documentation maintained for the corresponding 105 access requests.

- Assessed the sufficiency of the May 2019 periodic access review process for a random and judgmental sample of 4 of 23 divisions within Treasury and DTMB .

- Evaluated the appropriateness of users assigned elevated access rights for a judgmental sample of 6 of 58 instances occurring between June 2018 and August 2019.

- Evaluated logging and monitoring controls of security-related events.

- Evaluated controls over non-user accounts for a judgmental and random sample of 4 of 33 system accounts and 17 default user accounts as of August 19, 2019.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. For our judgmental samples, we could not project our results to the respective populations.

OBJECTIVE #2

To assess the sufficiency of selected tax processing controls within MIITAS.

To accomplish this objective, we:

- Judgmentally sampled and reviewed interface design documentation and reconciliation procedures for 11 of 59 system interfaces as of May 20, 2019 for compliance with industry best practices.

- Reconciled interfaced data for a judgmental sample of 11 of 59 system interfaces as of May 20, 2019. We also evaluated the reconciliation performed by Treasury and DTMB and assessed the sufficiency of supporting documentation maintained.

- Judgmentally and randomly sampled 43 of 17,719,483 tax return forms processed by MIITAS between January 1, 2018 and July 23, 2019 and validated that selected tax processing rules functioned in accordance with system specifications.

- Evaluated overall processing results of selected tax processing rules in accordance with system specifications.

- Analyzed the completeness and accuracy of selected tax processing data.

Our random sample was selected to eliminate any bias and enable us to project the results to the population. For our judgmental samples, we could not project our results to the respective populations.

OBJECTIVE #3

To assess the effectiveness of Treasury and DTMB's change controls over MIITAS.

To accomplish this objective, we:

- Reviewed a random sample of 12 of 119 system changes, including break-fixes and minor system enhancements, implemented from June 2018 through May 2019 for compliance with the State's change management policies and procedures.

- Randomly sampled 12 of 111 canceled system changes from June 2018 through May 2019 to evaluate the appropriateness of the change cancellation decision.

- Reviewed a judgmental sample of 2 of 15 completed system development projects implemented from June 2018 through May 2019 for compliance with the State's change management policies and procedures.

Our random samples were selected to eliminate bias and enable us to project the results to the respective populations. For our judgmental samples, we could not project our results to the respective populations.

CONCLUSIONS

We base our conclusions on our audit efforts and any resulting material conditions or reportable conditions.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve State government operations. Consequently, we prepare our performance audit reports on an exception basis.

CONFIDENTIAL AND SENSITIVE INFORMATION

Because of the confidentiality of MIITAS security configuration parameters, we summarized our testing results for presentation in the report and provided the underlying details to Treasury and DTMB management.

AGENCY RESPONSES

Our audit report contains 6 findings and 6 corresponding recommendations. Treasury and DTMB's preliminary response indicates that they agree with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion at the end of our fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

GLOSSARY OF ABBREVIATIONS AND TERMS

access controls

Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.

authorization object

Logical template containing one or more fields that are referenced by authority-check statements, which are coded into ABAP (Advanced Business Application Programming) programs to implement access restrictions in SAP.

availability

Timely and reliable access to data and information systems.

baseline configuration

A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed upon at a given point in time and that can be changed only through change control procedures.

change controls

Controls that ensure that program, system, or infrastructure modifications are properly authorized, tested, documented, and monitored.

confidentiality

Protection of data from unauthorized disclosure.

configuration checklist

Common security configurations that provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific IT platforms/products and instructions for configuring those information system components to meet operational requirements. Configuration checklists are also referred to as security configuration checklists, lockdown and hardening guides, security referenced guides, and security technical implementation guides.

DTMB

Department of Technology, Management, and Budget.

effectiveness

Success in achieving mission and goals.

Federal Information System Controls Audit Manual (FISCAM)

A methodology published by the U.S. Government Accountability Office (GAO) for performing information system control audits of federal and other governmental entities in accordance with *Government Auditing Standards.*

integrity

Accuracy, completeness, and timeliness of data in an information system.

interface controls

Controls that ensure the accurate, complete, and timely processing of data exchanged between information systems.

IRS

Internal Revenue Service.

JPMC

JPMorgan Chase.

material condition

A matter that, in the auditor's judgment, is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program. Our assessment of materiality is in relation to the respective audit objective.

MIITAS

Michigan Integrated Tax Administration System.

MTO

Michigan Taxpayers Online.

National Institute of Standards and Technology (NIST)

An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.

performance audit

An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision-making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.

principle of least privilege

The practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.

reportable condition

A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.

SAPGUI

SAP graphical user interface where software is installed on a user's workstation to access system functionality over the network.

security

Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.

segregation of duties

Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.

SOM

State of Michigan.

State Unified Information Technology Environment (SUITE)

A DTMB initiative to standardize methodologies, procedures, training, and tools for project management and system development throughout the executive branch of State government.

Statewide Integrated Governmental Management Applications (SIGMA)

The State's enterprise resource planning business process and software implementation that support budgeting, accounting, purchasing, human resource management, and other financial management activities.

threat

An activity, intentional or unintentional, with the potential for causing harm to an automated information system or activity.

transaction code

The letters and/or numbers entered into an SAP system command prompt to allow a user to access functions or programs.

Treasury

Department of Treasury.

vulnerability

Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

OAG

Office of the Auditor General

Independent Objective Transparent

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud
Hotline: (517) 334-8060, Ext. 1650