Office of the Auditor General

Follow-Up Report on Prior Audit Recommendations

Michigan Integrated Tax Administration System

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

September 2025

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

271-0595-19F

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

Follow-Up Report
Michigan Integrated Tax Administration System
Department of Treasury (Treasury) and Department of Technology, Management, and Budget (DTMB)

Report Number:
271-0595-19F

Released:
September 2025

We conducted this follow-up to determine whether Treasury and DTMB had taken appropriate corrective measures in response to the two material conditions noted in our March 2020 audit report.

Prior Audit Information	Follow-Up Results		
	Conclusion	**Finding**	**Agency Preliminary Response**
Finding 1 - Material condition Monitoring of security-related events needed. Agency agreed.	Partially complied	Reportable condition exists. See Finding 1.	Agrees
Finding 2 - Material condition Effective access controls not established and implemented. Agency agreed.	Partially complied	Reportable condition exists. See Finding 2.	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

This Page Left Intentionally Blank

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

September 3, 2025

Rachael Eubanks
State Treasurer
Richard H. Austin Building
Lansing, Michigan

Michelle Lange, Director
Department of Technology, Management, and Budget
and
Laura Clark, Chief Information Officer
Department of Technology, Management, and Budget
Elliott-Larsen Building
Lansing, Michigan

State Treasurer Eubanks, Director Lange, and Chief Information Officer Clark:

This is our follow-up report on the two material conditions (Findings 1 and 2) and two corresponding recommendations reported in the performance audit of the Michigan Integrated Tax Administration System, Department of Treasury and Department of Technology, Management, and Budget. That audit report was issued and distributed in March 2020. Additional copies are available on request or at audgen.michigan.gov.

Your agencies provided preliminary responses to the follow-up recommendations included in this report. 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 our follow-up. If you have any questions, please call me or Laura J. Hirst, CPA, Deputy Auditor General.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

MICHIGAN INTEGRATED TAX ADMINISTRATION SYSTEM

INTRODUCTION, PURPOSE OF FOLLOW-UP, AND SYSTEM DESCRIPTION

INTRODUCTION

This report contains the results of our follow-up of the two material conditions* (Findings 1 and 2) and two corresponding recommendations reported in our performance audit* of the Michigan Integrated Tax Administration System (MIITAS), Department of Treasury (Treasury) and Department of Technology, Management, and Budget (DTMB), issued in March 2020.

PURPOSE OF FOLLOW-UP

To determine whether Treasury and DTMB had taken appropriate corrective measures to address our corresponding recommendations.

SYSTEM DESCRIPTION

Treasury and DTMB implemented MIITAS to administer the following taxes:

- City of Detroit individual income, withholding, and corporate taxes.
- Corporate income tax.
- Essential Services Assessment.
- Flow-through entity tax.
- Marihuana retailers excise tax.
- Michigan business tax.
- Sales, use, and withholding taxes.

SAP software provides MIITAS's core tax processing functionality using the Tax and Revenue Management solution. Approximately 605 State employees and contractors access MIITAS and in fiscal year 2024, Treasury administered $29.9 billion in associated tax revenues.

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

PRIOR AUDIT FINDINGS AND RECOMMENDATIONS; AGENCY PLAN TO COMPLY; AND FOLLOW-UP CONCLUSIONS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

FINDING 1

Audit Finding Classification: Material condition.

Summary of the March 2020 Finding:
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*.

Recommendation Reported in March 2020:
We recommended Treasury, in conjunction with DTMB, monitor security-related events within MIITAS to help facilitate the ongoing awareness of threats, vulnerabilities, and information security.

AGENCY PLAN TO COMPLY*

On June 4, 2020, Treasury and DTMB stated they 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 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. A feasibility study will be conducted and completed by July 1, 2020 to determine which procedures will be supported by available resources.

FOLLOW-UP CONCLUSION

Partially complied. A reportable condition* exists.

Our follow-up noted Treasury and DTMB made significant progress in strengthening their access controls* through the implementation of improved business processes and the GRC tool. However, Treasury and DTMB should continue to improve monitoring of security-related events. Specifically, Treasury and DTMB did not appropriately monitor:

- Users identified by the GRC tool with segregation of duties* conflicts.
- User's activities when they obtain temporary elevated rights.
- Access rights granted outside of the GRC tool.

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

FOLLOW-UP RECOMMENDATION

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

FOLLOW-UP AGENCY PRELIMINARY RESPONSE

Treasury and DTMB provided us with the following response:

Treasury and DTMB agree with the recommendation.

Treasury and DTMB implemented the GRC solution in 2019 to more effectively and efficiently administer security for the MIITAS application (as noted in finding 2). We also created a monitoring plan that we continue to update as new risks are identified either through the GRC solution or performing risk assessments.

While stronger preventative controls significantly mitigate risk, it does not eliminate the need to continue to monitor. Treasury will continue to refine the monitoring plan to further address risk.

FINDING 2

Audit Finding Classification: Material condition.

Summary of the March 2020 Finding:
Treasury did not fully establish and implement effective access controls over MIITAS to help ensure data is secure and system controls are operating as intended.

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 92 users had access to these transaction codes.

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

   (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 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 723 users had access to these authorization objects.

   (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.

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

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

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

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

c. Treasury should improve its periodic access review process.

We randomly and judgmentally sampled 4 (17%) of 23 divisions within Treasury and DTMB to assess the May 2019 review process results. We noted 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'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 access is appropriately segregated to reduce security risks.

e. Treasury should improve its documentation of user access.

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.

Recommendation Reported in March 2020:
We recommended Treasury fully establish and implement effective access controls over MIITAS to help ensure data is secure and system controls are operating as intended.

AGENCY PLAN TO COMPLY

On June 4, 2020, Treasury stated it was aware of weaknesses with access control processes and initiated a project in 2018 to select and implement a 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.

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

   The GRC tool requires justification for the needed access as well as requiring approvals from the appropriate business owner as well as the security administrator before allowing a user to have access. The GRC tool also allows Treasury to set an end date for temporary access, which limits the risk of access no longer being needed. The emergency access management module of the GRC tool has been implemented and high-risk transaction codes identified by Treasury are being moved into roles that are used on a limited basis. This process is expected to be completed by June 2020. In addition, Treasury is completing a segregation of duties risk analysis leveraging the SAP GRC tool which will allow Treasury to better limit and remove access which is considered to be high-risk. The risk analysis is expected to be completed by July 2020.

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

   Treasury has reviewed the non-user accounts that were questioned during the audit and locked all non-user accounts where feasible. Treasury is currently reviewing other non-user accounts that are currently being used in MIITAS and determining the appropriate access. This process requires more extensive testing as removing access from the non-user accounts may cause inadvertent issues within MIITAS including system outages. A plan for restricting access for these non-user accounts will be developed and implementation will begin by the end of June 2020.

c. Treasury should improve its periodic access review process.

The GRC tool significantly reduced the manual work that was previously required to remove access from multiple environments. Treasury also increased its MIITAS monitoring staff to reduce the risk that user access is not removed timely. We consider this part of the finding to be complied with.

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

   Treasury is completing a segregation of duties risk analysis leveraging the SAP GRC tool which will automatically alert security administrators of MIITAS users with incompatible roles. The risk analysis is expected to be completed by July 2020.

e. Treasury should improve its documentation of user access.

   Treasury continues to train security liaisons about adequate supporting rationale for requesting access to MIITAS. In addition, the GRC tool requires the necessary approvals prior to allowing access to MIITAS which replaces the previous manual process. We consider this part of the finding to be complied with.

FOLLOW-UP CONCLUSION

Partially complied. A reportable condition exists.

Our follow-up noted Treasury made significant progress in strengthening its access controls through the implementation of improved business processes and the GRC tool. However, Treasury should continue to improve access controls over MIITAS to help ensure data is secure and system controls are operating as intended.

a. Partially complied.

   Treasury should continue to improve its management of high-risk access within MIITAS in accordance with Treasury policy ET-03179. We noted:

   (1) 7 (7%) of 97 judgmentally selected users with selected high-risk transaction codes and authorization objects had privileges not appropriate for their job responsibilities.

   (2) Treasury appropriately approved, documented, and removed elevated rights for all randomly sampled instances of elevated access assigned to users.

b. Complied.

Treasury implemented effective controls over non-user accounts.

We judgmentally and randomly sampled 5 of 23 system accounts and determined all were assigned an account manager and had a business reason for the level of access. Also, we reviewed 17 default user accounts and determined they were appropriately restricted.

c. Not complied.

Treasury should improve its periodic access review process.

We randomly and judgmentally sampled 5 of 22 divisions to assess the November 2024 MIITAS periodic review process. We noted 1 (20%) of 5 sampled divisions did not remove inappropriate user access.

d. Partially complied.

Treasury should continue to improve its segregation of duties over incompatible job functions.

Treasury implemented the GRC tool to prevent and detect segregation of duties violations for standardized roles in SAP. However, Treasury did not assess its customized roles to determine whether segregation of duties violations would occur if combinations of these roles were assigned.

e. Complied.

Treasury improved its documentation of user access.

We reviewed 16 of 143 user access requests with access granted between May 1, 2024 and May 19, 2025. We noted all 16 user access requests contained adequate information to support the level of access being requested and were properly approved.

FOLLOW-UP RECOMMENDATION

We recommend Treasury continue to improve access controls over MIITAS to help ensure data is secure and system controls are operating as intended.

FOLLOW-UP AGENCY PRELIMINARY RESPONSE

Treasury provided us with the following response:

Treasury agrees with the recommendation.

Treasury and DTMB implemented the GRC solution in 2019 to more effectively and efficiently administer security for the MIITAS application. As noted in the finding, Treasury has made *significant progress in reducing the risk of inappropriate access to data. Treasury will continue to assess these controls to ensure they are operating as intended to further reduce risk.*

FOLLOW-UP METHODOLOGY, PERIOD, AND AGENCY RESPONSES

METHODOLOGY

We reviewed Treasury and DTMB's corrective action plan and procedures and interviewed Treasury and DTMB personnel. Specifically, for:

- Finding 1, we evaluated logging and monitoring controls in SAP, as of May 2025, over:
    - Segregation of duties conflicts identified by the GRC tool.
    - Activities performed by users with temporary elevated access rights.
    - Whether access rights were granted outside of the GRC tool.
- Finding 2, we:
    - Judgmentally selected 114 transaction codes and 17 authorization objects as of May 2025 and evaluated the appropriateness of 97 users assigned access.
    - Randomly sampled 2 of 5 instances occurring between May 1, 2024 and June 1, 2025 and evaluated the appropriateness of users assigned elevated access rights.
    - Randomly and judgmentally sampled 5 of 23 system accounts as of May 19, 2025 and 17 default user accounts as of June 3, 2025 to evaluate the appropriateness of access rights for non-user accounts.
    - Randomly and judgmentally sampled 5 of 22 divisions and assessed the sufficiency of the November 2024 periodic access review process.
    - Evaluated the design and implementation of Treasury's segregation of duties access controls.
    - Randomly and judgmentally selected 16 of 143 users created in MIITAS between May 1, 2024 and May 19, 2025 to determine whether access requests:
        - Identified a reason to support the access being requested.
        - Were appropriately approved.

PERIOD

Our follow-up generally covered May 2024 to June 2025.

AGENCY RESPONSES

Our follow-up report contains 2 recommendations. Treasury and DTMB's preliminary response indicate they agree with 1 recommendation, and Treasury indicates it agrees with 1 recommendation.

The agency preliminary response to each follow-up 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 3, 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 protecting data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.

agency plan to comply

The response required by Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 3, Section 100). The audited agency is required to develop a plan to comply with Office of the Auditor General audit recommendations and to submit the plan 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.

authorization object

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

DTMB

Department of Technology, Management, and Budget.

GRC

Governance, Risk, and Compliance.

material condition

A matter, in the auditor's judgment, which 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.

performance audit

An audit which 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.

reportable condition A matter, in the auditor's judgment, less severe than a material condition and falls within any of the following categories: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud.

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.

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.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

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) 334-8070