Office of the Auditor General
Performance Audit Report

AASHTOWare Project Construction and Materials

Michigan Department of Transportation and
Department of Technology, Management, and Budget

January 2024

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

591-0591-23

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

Office of the Auditor General

Report Summary

Performance Audit

AASHTOWare Project Construction and Materials (APCM)
Michigan Department of Transportation (MDOT) and Department of Technology, Management, and Budget (DTMB)

Report Number:
591-0591-23

Released:
January 2024

MDOT manages the life cycle of the construction project beginning with initial project design and specifications, continuing through the bid letting and contract award process, and ending with the execution of the job site construction activities. The current software suite manages a majority of the construction contracts and processes over $1.9 billion in construction project payments.

Because MDOT plans to sunset the current software suite, it began using AASHTOWare Project. MDOT uses two of the AASHTOWare Project modules: APCM and AASHTOWare Project Preconstruction. This audit focused on the APCM module, which documents the daily project work and compiles the biweekly payments to construction contractors. As of June 13, 2023, APCM managed approximately $144 million in construction contracts and had approximately 500 users. MDOT's long-term goal is for APCM to manage all construction contracts and payments.

Audit Objective	Conclusion
Objective 1: To assess the effectiveness of selected APCM access controls.	Not effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
MDOT's monitoring of user access excluded 67% of APCM users. Also, access was not removed for 49% of users with inactivity greater than a year, and 83% of transferred or terminated State of Michigan users did not have access removed timely (Finding 1).	X		Agrees
Of sampled users, 70% did not have user access forms and for those with forms, 100% lacked approved access documentation. Also, MDOT granted 11% of the sampled high-risk users inappropriate access and had not defined incompatible user roles (Finding 2).	X		Agrees

<table>
<tr><th colspan="3">Audit Objective</th><th>Conclusion</th></tr>
<tr><td colspan="3">Objective 2: To assess the effectiveness of MDOT and DTMB's efforts to implement controls over APCM interfaces.</td><td>Effective</td></tr>
<tr><th>Findings Related to This Audit Objective</th><th>Material Condition</th><th>Reportable Condition</th><th>Agency Preliminary Response</th></tr>
<tr><td>None reported.</td><td colspan="3">Not applicable.</td></tr>
</table>

<table>
<tr><th colspan="3">Audit Objective</th><th>Conclusion</th></tr>
<tr><td colspan="3">Objective 3: To assess the effectiveness of MDOT and DTMB's efforts to implement change controls over the APCM application and data.</td><td>Effective</td></tr>
<tr><th>Findings Related to This Audit Objective</th><th>Material Condition</th><th>Reportable Condition</th><th>Agency Preliminary Response</th></tr>
<tr><td>MDOT and DTMB did not maintain documentation for 95% of system integration testing, 97% of user acceptance testing, and 100% of post-implementation validation (Finding 3).</td><td></td><td>X</td><td>Disagrees</td></tr>
</table>

<table>
<tr><th colspan="3">Audit Objective</th><th>Conclusion</th></tr>
<tr><td colspan="3">Objective 4: To assess the sufficiency of MDOT's efforts to ensure the accuracy of construction records within APCM.</td><td>Sufficient</td></tr>
<tr><th>Findings Related to This Audit Objective</th><th>Material Condition</th><th>Reportable Condition</th><th>Agency Preliminary Response</th></tr>
<tr><td>None reported.</td><td colspan="3">Not applicable.</td></tr>
</table>

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

Doug A. Ringler, CPA, CIA
Auditor General

January 12, 2024

Michael D. Hayes, Chair
State Transportation Commission
and
Bradley C. Wieferich, PE, Director
Michigan Department of Transportation
Murray D. Van Wagoner 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

Chair Hayes, Director Wieferich, Director Lange, and Chief Information Officer Clark:

This is our performance audit report on the AASHTOWare Project Construction and Materials, Michigan Department of Transportation 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

AASHTOWARE PROJECT CONSTRUCTION AND MATERIALS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

ACCESS CONTROLS

BACKGROUND

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

The primary users of the AASHTOWare Project Construction and Materials* (APCM) module consist of Michigan Department of Transportation (MDOT), consultant, local agency, and contractor staff. MDOT utilizes an interactive access request form to determine which of the 61 available roles to grant to users. The form is coded to automatically populate the role assignment which should be granted based on the user responses for job function, organization type, and signature authority fields of the form.

As of July 12, 2023, 521 active users accessed the APCM module.

AUDIT OBJECTIVE

To assess the effectiveness* of selected APCM access controls.

CONCLUSION

Not effective.

FACTORS IMPACTING CONCLUSION

- Two material conditions* related to improving APCM user access monitoring (Finding 1) and fully establishing and implementing APCM user access controls (Finding 2).

- MDOT had established and implemented some user access controls within APCM in accordance with State policy, such as defining processes for requesting and approving user access, conducting semiannual user certifications, and notifying the data custodian of departed users.

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

FINDING 1

Improvements to user access monitoring needed.

MDOT should improve its monitoring over APCM user accounts to ensure access remains appropriate. Ineffective monitoring of access rights increases the risk of unauthorized access, use, and modification of APCM data.

State of Michigan (SOM) Technical Standard 1340.00.020.01 requires State agencies to conduct semiannual and annual certifications for privileged accounts and non-privileged accounts to verify accounts are still required and compliant with the account settings and access permissions. The Standard also requires the information systems automatically disable user accounts after 60 days of inactivity. However, MDOT has a documented business need to allow user access to remain enabled until 365 days of inactivity. In addition, the Standard requires State agencies to remove user access within 3 business days when accounts are no longer required and when users are terminated or transferred.

The National Institute of Standards and Technology* (NIST) Special Publication 800-53 recommends disabling expired, inactive, or otherwise anomalous accounts to support the concepts of least privilege and least functionality which reduce the attack surface of the system.

MDOT performs semiannual certification of APCM users whose log-in activity is greater than 180 days. We reviewed the most recent semiannual certification conducted on April 28, 2023, which included 233 APCM users who accessed the application with 345 APCM user roles. Our review disclosed MDOT did not ensure:

a. Certifications were conducted for all user accounts. The report used to conduct the certification review excluded:

67% of APCM users were not included in the annual certification.

(1) 351 (67%) of the 521 users who as of July 12, 2023 accessed the application within 180 days.

(2) 440 users who were granted access to APCM and never accessed the application or were not assigned roles.

b. User accounts were disabled because of inactivity for greater than 365 days. APCM does not automatically disable inactive user accounts. We noted access was not disabled for:

Access was not removed for 49% of inactive users.

(1) 114 (49%) of the 233 APCM users. In addition, 354 users who were granted access to APCM never accessed the application or were not assigned roles.

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

(2) 176 (51%) of the 345 APCM user roles. The table below shows when user roles were last accessed:

Last Log-In Date	Number of Active APCM User Roles
Between 1 to 2 years ago	80
Between 2 to 3 years ago	31
Between 3 to 4 years ago	30
Between 4 to 5 years ago	31
Over 5 years ago	4
Total	176

MDOT policy requires account deactivation upon receiving a biweekly notification of accounts which are no longer required and when users are terminated or transferred. We noted MDOT did not ensure:

Access was not removed timely.

c. Removal of access for all terminated or transferred users. We reviewed all APCM users who accessed the application as of July 12, 2023, which included 324 SOM users. We noted access was not disabled for:

(1) 18 (6%) users who departed SOM employment between 47 and 1,572 days ago.

(2) 3 (1%) users who potentially transferred from MDOT to other departments.

(3) 6 (2%) users whom MDOT could not identify.

d. Timely removal of access. We reviewed all 136 users with disabled access as of July 21, 2023 and noted:

(1) 113 (83%) users departed SOM employment between 21 and 3,055 days prior to the date access was disabled.

(2) 9 (7%) users whom MDOT could not identify.

MDOT informed us that because of the cyclical nature of construction in Michigan, it is burdensome to remove user access as it may be needed on a future construction project.

We consider this finding to be a material condition because of the considerable exception rate of inactive users and the number of users not reviewed in the user certification.

RECOMMENDATION

We recommend MDOT improve its monitoring over APCM user accounts to ensure access remains appropriate.

AGENCY PRELIMINARY RESPONSE

MDOT provided us with the following response:

MDOT agrees with the recommendation. MDOT will work with DTMB and the software vendor to develop a custom system process to automatically deactivate inactive accounts. The process will be developed and implemented by June 2024.

FINDING 2

Effective access controls not fully established and implemented.

MDOT did not fully establish and implement effective access controls over APCM, increasing the risk of unauthorized access, use, and modification of APCM data.

SOM Technical Standard 1340.00.020.01 requires State agencies to establish a process to control and document the assignment of access rights based on current job responsibilities and the principle of least privilege*. Also, SOM Technical Standard 1340.00.020.03 requires State agencies to maintain documentation of authorized users from the initial request for creation of user ID and access to the final de-registration of users. In addition, the Federal Information System Controls Audit Manual* (FISCAM) recommends an entity-wide policy outlining the responsibilities of group and related individuals pertaining to incompatible activities be documented, communicated, and enforced.

Our review of APCM access controls disclosed:

70% of sampled users did not have user access forms. Also, 11% of the sampled high-risk users were granted inappropriate access.

a. MDOT had incomplete documentation for granting user access. We selected a sample of 33 users, including 9 judgmentally selected high-risk users and 24 randomly selected non-high-risk users who accessed APCM. MDOT did not collect or maintain user access forms for 23 (70%) of the 33 users. For the 10 users with user access forms, we noted:

   (1) 10 (100%) users did not have documented approval for the access granted.

   (2) 2 (20%) users were granted access with incomplete forms.

   (3) 2 (20%) users were granted additional roles beyond the documented request form.

b. MDOT unnecessarily granted administrator access rights to 1 (11%) of 9 high-risk users. Applying the principle of least privilege helps to minimize the security impact of a failure, corruption, or misuse of APCM. We identified a weakness in the annual certification process that contributed to the exception noted in this finding (see Finding 1, part a. (1)).

c. MDOT did not identify incompatible roles within APCM. Identifying incompatible functions is a key control in effective segregation of duties*. Conversely, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed. MDOT should limit access rights for users to perform their necessary day-to-day tasks to reduce the potential of inappropriate use.

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

> MDOT utilizes user access request forms to create users in APCM based on the requestor's job function, organization type, and signature authority. The APCM user access forms are designed to eliminate the possibility of incompatible roles being assigned. However, we noted 2 users approved 21 of their own daily work reports* (DWRs) during our audit period. DWRs directly impact pay estimates to contractors, which then results in a payment to the contractor.

As the application owner, MDOT did not ensure compliance with SOM technical standards and implement FISCAM practices to accurately document and grant user access. MDOT informed us internal users were not required to complete the access request forms; however, as of June 23, 2023, MDOT implemented a new process of requesting and granting user access for all users.

We consider this finding to be a material condition because of the considerable exception rate of incomplete access forms and lack of user access documentation. In addition, the potential risk of inappropriate payments to contractors resulting from a lack of segregation of duties between the DWRs' submitters and approvers.

RECOMMENDATION

We recommend MDOT fully establish and implement effective application access controls over APCM.

AGENCY PRELIMINARY RESPONSE

MDOT provided us with the following response:

MDOT agrees with the recommendation. MDOT is in the process of testing APCM release 5.00 for implementation, and this release will restrict access for users to approve their own daily work reports (DWRs). MDOT will also create a list of incompatible roles and report(s) for use during the user account certification. In addition, from a technical and best practice standpoint, MDOT will implement SOM technical security standards. MDOT expects completion by June 2024.

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

INTERFACE CONTROLS

BACKGROUND

Interface controls* ensure the accurate, complete, and timely processing of data exchanged between information systems.

APCM utilizes accessible views* with 20 of the other MDOT applications. Accessible views allow users of other applications to view information in the AASHTOWare database without transferring data.

Also, APCM utilizes a traditional interface with the Statewide Integrated Governmental Management Applications* (SIGMA). In fiscal year 2022, the interface between APCM and SIGMA processed 636 payment estimate vouchers with a total amount of $56.5 million in construction expenditures.

MDOT performs daily reconciliations to ensure all APCM expenditures are transferred accurately and completely to SIGMA.

AUDIT OBJECTIVE

To assess the effectiveness of MDOT and the Department of Technology, Management, and Budget's (DTMB's) efforts to implement controls over APCM interfaces.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- MDOT and DTMB established and implemented interface policies, procedures, and strategies that generally complied with industry best practices.

- For 100% of dates reviewed for batch interfaces, payment vouchers were successfully transferred to SIGMA.

- For 100% of dates reviewed for point-to-point interfaces, bid letting* information was successfully transferred.

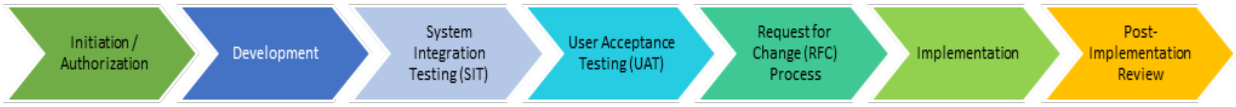
- MDOT timely followed up on and corrected identified interface errors.

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

CHANGE CONTROLS

BACKGROUND

Changes to APCM are typically initiated when MDOT authorizes a needed modification. DTMB constructs the change in a development environment moving to a test environment where the change undergoes various quality assurance processes, such as system integration testing (SIT) and user acceptance testing (UAT). Upon completion of testing, MDOT authorizes DTMB to move the change into the production environment. After production implementation, MDOT conducts a post-implementation review to verify the change met user expectations.


Initiation / Authorization
Development
System Integration Testing (SIT)
User Acceptance Testing (UAT)
Request for Change (RFC) Process
Implementation
Post-Implementation Review

APCM changes generally consist of system upgrades, implementation of new programs, and correction of programming errors.

AUDIT OBJECTIVE

To assess the effectiveness of MDOT and DTMB's efforts to implement change controls over the APCM application and data.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- MDOT and DTMB have established and implemented change management procedures and workflow in accordance with SOM policies, standards, and procedures.
- MDOT and DTMB had authorizations and approvals of the initiation, testing, implementation, and post-implementation phases of the change management process.
- One reportable condition* related to MDOT and DTMB lacking testing documentation of SIT, UAT, and post-implementation review (Finding 3).

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

FINDING 3

Improvements needed to document change control activities.

MDOT, in conjunction with DTMB, did not maintain documentation of control activities performed during the change management life cycle to help ensure all changes to APCM were properly tested, implemented, and reviewed.

SOM Technical Procedure 1340.00.060.04.01 requires the:

- Quality assurance team to perform SIT and document the results.

- Business owner to perform UAT to ensure system changes meet the requirements by testing against test plans and documenting the results.

- Business owner to perform post-implementation validation of system changes.

MDOT and DTMB utilize Solutions Business Manager Suite (SBMS) as a change management software tool to manage changes made to APCM. SBMS is configured to have a designed workflow requiring approvals for each step of the change management life cycle.

We reviewed the 29 changes MDOT and DTMB initiated and completed to APCM between October 1, 2021 and July 20, 2023. Based on the nature of the change, some audit procedures were not applicable to all 29 changes. Our review disclosed MDOT did not:

a. In conjunction with DTMB, maintain documentation of SIT for 20 (95%) of 21 changes. SIT helps to ensure new software code will not impact existing APCM functionalities and the updated functionalities meet the design of APCM. Although SIT approvals occurred and moved the change forward in the workflow, maintaining SIT results helps facilitate fixing system errors and helps aid in future quality enhancements.

b. Maintain documentation of UAT for 28 (97%) of the 29 changes. UAT helps to verify system changes are working as intended and reduces any unintended consequences prior to production implementation. Although UAT approvals occurred and moved the change forward in the workflow, maintaining UAT results helps provide details of potential defects and steps to reproduce testing for post-implementation review.

c. Maintain documentation of post-implementation validation for 29 (100%) of the 29 changes. Post-implementation validation helps ensure production changes are applied and function as intended. Although approvals noted post-implementation validation occurred and moved the change forward in the change management workflow, maintaining results of post-implementation validation helps produce audit trails of application changes.

Although we identified a significant number of errors related to the lack of documentation, we noted evidence of business owner involvement at appropriate phases of the change management life cycle.

MDOT and DTMB informed us it did not maintain documentation to support all phases of the change management life cycle because of the assumption that approvals satisfied the intent of the established SOM Enterprise Change Management Procedure for documenting SIT testing, UAT testing, and post-implementation validation.

RECOMMENDATION

We recommend MDOT, in conjunction with DTMB, maintain documentation of control activities performed during the change management life cycle to help ensure all changes to APCM are properly tested, implemented, and reviewed.

AGENCY PRELIMINARY RESPONSE

MDOT and DTMB disagree. Given the length of MDOT and DTMB's preliminary response, the response and our auditor's comments to Finding 3 are presented on page 19.

CONSTRUCTION RECORDS

BACKGROUND

Validation rules* are a control technique used to provide reasonable assurance transactions are accurately and properly recorded with the correct data.

APCM contains 26 unique validation rule types to determine whether information may be entered into the module. Over 4,200 validation rules are within the 2,627 unique fields to ensure the accuracy of application records. Validation rules use programming logic to determine whether data entered aligns with the validation rule. If data does not align with the validation rule, the data cannot be entered into APCM.

AUDIT OBJECTIVE

To assess the sufficiency of MDOT's efforts to ensure the accuracy of construction records within APCM.

CONCLUSION

Sufficient.

FACTORS IMPACTING CONCLUSION

- MDOT implemented effective validation rules ensuring data manually entered and interfaced into APCM is accurate.

- No identified instances of incomplete or inaccurate data in APCM related to inbound data from construction contracts or select external databases.

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

Finding 3 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains MDOT and DTMB's preliminary response to Finding 3 and our auditor's comments providing further clarification and context where necessary.

Finding 3: Improvements needed to document change control activities.

MDOT and DTMB provided us with the following response:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
MDOT and DTMB disagree that appropriate documentation was not maintained for control activities performed during the change management life cycle. Appropriate and pertinent documentation was maintained. State of Michigan policy 1360.00, Systems Engineering Methodology, requires all state agencies to follow the Systems Engineering Methodology (SEM).	SOM Administrative Guide to State Government policy 1340 establishes the strategic view of IT security for information systems that process, store, and transmit SOM information, as well as establish the corresponding standards and procedures for the individuals who implement and manage information systems. The SOM Enterprise Change Control Standard (1340.00.060.04) protects the integrity of the environment by planning, documenting, and approving changes to anything that could have an adverse effect on IT services. The Systems Engineering Methodology (SEM) is just that, a methodology, and does not supersede the standard and procedures above. The SOM Enterprise Change Control Procedure (1340.00.060.04.01) requires the testing results to be documented, in addition to the approvals, which is above and beyond what the SEM requires. Therefore, appropriate and pertinent information was not maintained.
As referenced in the audit report, the OAG reviewed 29 changes. DTMB and MDOT confirmed these changes are categorized as system maintenance according to the SEM, and the systems maintenance process is for projects under 200 hours. The SEM states: "To the extent possible, all maintenance and operations activities should be managed as a project, utilizing the Systems Maintenance Template (SEM-0931), to gain the benefits inherent in project management and to enable tracking of activities and costs. The extent of project management activity will vary, and should be tailored according to size, complexity, and impact of the change or enhancement."	We reviewed the SEM-0931 form and provided DTMB and MDOT feedback on our review of the methodology. We noted the form does not align with SOM Enterprise Change Control Procedure requirements (1340.00.060.04.01) because they only require documenting errors. While the form only requires an approval, the procedure requires documented testing results and is applicable to all SOM applications and databases, with no exclusions for maintenance.

In addition, the SEM refers to the System Maintenance Guidebook (SMG), which provides information on maintenance projects and further supports the requirements. The SMG documents each system maintenance stage including the testing stage and contains a detailed description of the System Maintenance Document (SEM-0931). In addition, the SMG describes the outputs of a completed test as completion of the "Integration Test, System Test, and User Acceptance Test sections of the SEM-0931." Additionally, the review process for the testing stage is a structured walkthrough, which is documented in the SEM-0931.

For 100% (29 of 29) of the changes the OAG reviewed, SIT and UAT occurred using the tool equivalent of the SEM-0931. MDOT and DTMB provided the OAG a crosswalk of the SEM to the tool equivalent and demonstrated that it aligned with the SEM-0931. All required information was contained in the tool equivalent, and the approvals in the tool equivalent substantiated that testing was performed and completed.

The System Maintenance Guidebook (SMG) referred to in the SEM has no authoritative requirements and does not supersede the SOM technical standards and procedures. The SEM-0931 form does not align with SOM Enterprise Change Control Procedure requirements, therefore using a "tool equivalent of the SEM-0931" does not conform either. While we acknowledge approvals were obtained, supporting documentation such as the SIT and UAT testing results were not. This information is required by SOM procedures.

In alignment with SOM Technical Procedure 1340.00.060.04.01, post-implementation validation is verification that the installation was completed, changes were applied, and the change functioned as expected. Also, per the SEM, the minimum exit criteria for post deployment validation is "Product Owner and designated testers have concluded the system is ready for use by the intended audience." In addition, the approvals are documented on the SEM-0185 and SEM-0189 forms, which do not require testing or validation artifacts. Therefore, the tool equivalent in use contains all approvals from both DTMB and MDOT.

An approval does not show how the validation occurred, if requirements have been met, and if implemented changes are working as intended. These changes are occurring in the production environment and will have the greatest impact on the users. In addition, Control Objectives for Information and Related Technology* (COBIT) BAI 07.08 states that post implementation reviews identify, assess, and report the following events have occurred: enterprise requirements have been met; internal/external stakeholders expectations are met; and the change management processes were performed effectively.

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

SYSTEM DESCRIPTION

MDOT manages the life cycle of construction projects beginning with the initial project design and specifications, continuing through the bid letting and contract award process, and ending with the execution of the job site construction activities. The current software suite manages the majority of the construction contracts and processes over $1.9 billion in construction project payments.

Because MDOT plans to sunset the current software suite, it began using AASHTOWare Project. MDOT is using two of the AASHTOWare Project modules: APCM and AASHTOWare Project Preconstruction* (APPC). APCM documents the daily project work and compiles the biweekly payments to construction contractors. As of June 13, 2023, APCM managed approximately $144 million in construction contracts and had approximately 500 users. MDOT's long-term goal is for APCM to manage all future construction contracts and payments.

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

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine APCM records and processes related to access controls, interface controls, and change controls. 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 APPC component controls or DTMB operating system, database, and network controls. Therefore, we provide no conclusions related to these items.

As part of the audit, we considered the five components of internal control* (control environment, risk assessment, control activities, information and communication, and monitoring activities) relative to the audit objectives and determined all components were significant.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2021 through August 31, 2023.

METHODOLOGY

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

- Interviewed MDOT and DTMB staff to obtain an understanding of APCM and processes related to user access, interface, and change controls.
- Reviewed SOM policies, standards, procedures, and industry best practices related to MDOT and APCM.
- Analyzed contract values and expenditures.
- Obtained an understanding of MDOT and DTMB's key processes and internal control significant to the potential audit objectives.

OBJECTIVE 1

To assess the effectiveness of selected APCM access controls.

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

To accomplish this objective, we:

- Randomly and judgmentally sampled 33 of 521 APCM users who accessed the application as of July 12, 2023 to determine whether MDOT:
  - Maintained and approved access request forms.
  - Granted access to the APCM user roles requested on the access request forms.
  - Properly implemented principle of least privilege controls.
- Reviewed all 521 users who accessed APCM as of July 12, 2023, which included 324 SOM users, to determine whether the users were current MDOT or DTMB employees recorded in the State's Human Resources Management Network* as of July 17, 2023.
- Reviewed all 136 users with disabled access as of July 21, 2023 to determine whether effective controls were implemented to ensure terminated users were removed in a timely manner as required by SOM Technical Standard 1340.00.020.01.
- Reviewed MDOT's user certification conducted April 28, 2023 to evaluate its design and validate whether inactive APCM user accounts and user roles were disabled timely.
- Reviewed all 472 users created prior to MDOT's recertification conducted April 28, 2023 who had not accessed the application or were not assigned roles to validate whether inactive APCM user accounts were disabled timely.
- Interviewed MDOT staff to obtain an understanding of APCM incompatible roles.
- Reviewed DWRs submitted from October 1, 2021 to July 12, 2023 by 149 users assigned roles capable of approving DWRs to determine whether the users self-approved DWRs.
- Judgmentally sampled 2 of 12 read-only user roles as of June 9, 2023 and 374 services, which are actions the user can execute. We:
  - Judgmentally selected 53 services as of June 20, 2023 to determine whether the services allowed for more access than intended.

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

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. Our judgmental samples were selected based on risk and to ensure significant State government operations within the population were sufficiently reviewed. For our judgmental samples, we could not project the results to the respective populations.

OBJECTIVE 2

To assess the effectiveness of MDOT and DTMB's efforts to implement controls over APCM interfaces.

To accomplish this objective, we:

- Reviewed interface documents for compliance with industry best practices.

- We randomly sampled 10 of 76 batch interface dates from October 1, 2021 through June 8, 2023 and validated the files were retrieved and transferred to SIGMA.

- We tested all 14 point-to-point interface dates occurring within our audit period between October 1, 2021 and July 27, 2023 and validated the data was retrieved and transferred.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations.

OBJECTIVE 3

To assess the effectiveness of MDOT and DTMB's efforts to implement change controls over the APCM application and data.

To accomplish this objective, we:

- Compared MDOT and DTMB's change management process with the State's policies and procedures and industry best practices.

- Reviewed the 29 system changes MDOT and DTMB initiated and completed to APCM between October 1, 2021 and July 20, 2023 for compliance with the State's change management policies and procedures and industry best practices.

OBJECTIVE 4

To assess the sufficiency of MDOT's efforts to ensure the accuracy of construction records within APCM.

To accomplish this objective, we:

- Judgmentally sampled 40 of 131 fields within APCM as of June 20, 2023 to verify edit checks were operating as intended.

- Reviewed all 65 fields intended for viewing and editing by specific roles within APCM to verify they could be accessed appropriately by the applicable role.

- Randomly sampled 1 of 11 new contracts in APCM as of August 21, 2023 to determine whether MDOT accurately entered the data from the contract into APPC.

- Randomly sampled 10 of 54 ongoing projects in APCM as of August 29, 2023 to determine whether inbound data from JobNet*, the MDOT Architecture Project (MAP) Database*, and Phase Initiator* (PI) is complete and accurate in APPC.

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

AGENCY RESPONSES

Our audit report contains 3 findings and 3 corresponding recommendations. MDOT's preliminary response indicates it agrees with 2 recommendations, and MDOT and DTMB disagree with 1 recommendation.

The agency preliminary response following 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.

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

GLOSSARY OF ABBREVIATIONS AND TERMS

AASHTOWare Project Construction and Materials (APCM)
A software application used for documenting construction progress and for initiating contractor payments.

AASHTOWare Project Preconstruction (APPC)
A software application used in the early phases of a construction project including proposal preparation, bid based pricing, bid letting management, and proposal award.

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

accessible view
Utilizing Structured Query Language (SQL) queries to present a set of data from one application to another without transferring the data.

auditor's comments to agency preliminary response
Comments the OAG includes in an audit report to comply with *Government Auditing Standards*. Auditors are required to evaluate the validity of the audited entity's response when it is inconsistent or in conflict with the findings, conclusions, or recommendations. If the auditors disagree with the response, they should explain in the report their reasons for disagreement.

bid letting
The process of advertising projects open for bids, contractors submitting bids, and MDOT reviewing contractors' submitted bids for trunkline projects.

Control Objectives for Information and Related Technology (COBIT)
A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over IT.

daily work report (DWR)
A record of the daily activity at the job site.

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*.

Human Resources Management Network

The State's integrated human resources system that processes personnel, payroll, and employee benefits data.

ID

identification.

interface controls

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

internal control

The plan, policies, methods, and procedures adopted by management to meet its mission, strategic plan, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It also includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; violations of laws, regulations, and provisions of contracts and grant agreements; or abuse.

JobNet

A software application maintaining essential transportation project information and data for MDOT's personnel and local agency use.

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.

MDOT

Michigan Department of Transportation.

MDOT Architecture Project (MAP) Database

A database repository for MDOT's project, job, and phase information for local improvements receiving federal aid and for the trunkline capital improvement program.

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.

Phase Initiator (PI)
An application used to request initial obligation and obligation revisions for all phases of MDOT transportation projects and to track and monitor the financial closeout process of those projects.

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 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: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud.

SBMS
Solutions Business Manager Suite.

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.

SEM
Systems Engineering Methodology.

SIT
system integration testing.

SMG
System Maintenance Guidebook.

SOM
State of Michigan.

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.

UAT
user acceptance testing.

validation rule Control technique used to provide reasonable assurance transactions are accurately and properly recorded with the correct data.

This Page Left Intentionally Blank

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