Office of the Auditor General
Performance Audit Report

Statewide Change Management Controls
Department of Technology, Management, and Budget

May 2017

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

071-0520-16

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.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit

Statewide Change Management Controls

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0520-16

Released:
May 2017

Change management is the process of authorizing, testing, documenting, and monitoring modifications to the infrastructure or any aspect of IT services in a controlled and planned manner, enabling the implementation of changes with minimal disruption of operations. The State's change management process involves various DTMB teams, such as Agency Services and Data Center Operations. Between October 1, 2015 and March 31, 2016, approximately 9,300 changes and 1,300 requests for change were placed into production.

Audit Objective	Conclusion
Objective #1: To assess the sufficiency of DTMB's governance structure over change management processes related to the State's IT applications.	Sufficient, with exceptions

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB had not fully established comprehensive policies, standards, and procedures for its change management process. Lack of clear and comprehensive guidance resulted in reduced monitoring and oversight, lack of documentation supporting changes, and insufficient segregation of duties as further defined in Findings #2, #3, and #5 (Finding #1).	X		Agrees
DTMB did not effectively monitor its change management process to help reduce the risk that intentional or inadvertent changes would impair the proper functioning or integrity of the State's IT systems. DTMB had not assigned configuration management managers for 8 (47%) of the 17 executive branch departments (Finding #2).		X	Agrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of DTMB's efforts to implement change management controls over the State's IT applications.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
Documentation of key control activities were lacking throughout the change management lifecycle. For example, DTMB did not maintain documentation of the authorization to initiate or implement a change (for 36% and 26% of the changes selected, respectively) and did not maintain documentation of post-implementation testing for 56% of the changes selected. Also, key testing phase activities were lacking documentation for 26% to 77% of changes reviewed (Finding #3).		X	Agrees
DTMB did not consistently perform quality assurance testing (QAT) activities for 9 (53%) of the 17 executive branch departments. QAT helps ensure the quality of the change, that the change will work as designed, and that the change reflects business owner requirements (Finding #4).		X	Agrees
DTMB should improve the segregation of duties throughout the change management lifecycle to reduce the risk that unintended or unauthorized changes are implemented in the State's IT environment. We identified instances in which DTMB, instead of the business owner, performed authorization and testing duties and allowed developers to test and implement their own work (Finding #5).		X	Agrees
DTMB did not consistently create and maintain listings of persons authorized to approve changes at each phase of the change management lifecycle for 12 (71%) of the 17 executive branch departments (Finding #6).		X	Agrees
DTMB did not input all changes into the Service Management and Monitoring System to ensure that all changes were identified, authorized, and assessed for adverse impact on the State's IT environment prior to implementation. DTMB did not follow procedures for entering 57 (27%) of 209 changes reviewed (Finding #7).		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

May 9, 2017

Mr. David B. Behen
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Mr. Behen:

I am pleased to provide this performance audit report on Statewide Change Management Controls, Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agency 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 submit it within 60 days of the date above to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services 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

STATEWIDE CHANGE MANAGEMENT CONTROLS

	Page
Report Summary	1
Report Letter	3
Audit Objectives, Conclusions, Findings, and Observations	
Governance Structure	8
Findings:	
1. Policies, standards, and procedures need enhancement.	9
2. Monitoring controls need improvement.	12
Implementation of Change Management Controls	14
Findings:	
3. Evidence of control activities not consistently documented.	15
4. QAT not consistently performed.	17
5. Segregation of duties not always enforced.	19
6. Improvements to authorization process needed.	22
7. Use of SMMS should be enforced.	24
Description	26
Audit Scope, Methodology, and Other Information	28
Glossary of Abbreviations and Terms	30

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

GOVERNANCE STRUCTURE

BACKGROUND

The mission* of the Enterprise Service Operations Governance Board (ESOGB) is to produce, deliver, maintain, and audit the operational processes, policy, and procedures required to manage IT service operation processes that affect IT service delivery within the DTMB-controlled IT infrastructure. The ESOGB reviews Local Change Advisory Boards (LCABs) for consistency and develops policies for both LCAB and Enterprise Change Advisory Board (ECAB) workflow. Also, the ESOGB audits the LCABs annually for compliance.

Control Objectives for Information and Related Technology* (COBIT) and Information Technology Infrastructure Library* (ITIL) are frameworks adopted by the Department of Technology, Management, and Budget (DTMB) as best practices for IT management and governance.

AUDIT OBJECTIVE

To assess the sufficiency of DTMB's governance structure over change management processes related to the State's IT applications.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- DTMB established some policies and procedures related to change management.
- DTMB established the State Unified Information Technology Environment* (SUITE), which provides additional guidance related to change management.
- Several review boards (LCABs, ECAB, and ESOGB) facilitate and oversee the implementation of changes.
- One material condition* related to the enhancement of policies, standards, and procedures (Finding #1).
- One reportable condition* related to the improvement of monitoring controls (Finding #2).

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

FINDING #1

Policies, standards, and procedures need enhancement.

DTMB had not fully established comprehensive policies, standards, and procedures for its change management process. Lack of clear and comprehensive guidance resulted in reduced monitoring and oversight, lack of documentation supporting changes, and insufficient segregation of duties* as further defined in Findings #2, #3, and #5.

COBIT states that formal change management policies and procedures should be established to ensure that all modifications are handled in a standardized manner. Toward that end, DTMB established various policies, standards, and procedures and developed various SUITE manuals. However, DTMB could enhance these by providing better clarity and detailed guidance in areas, such as:

a. Identifying artifacts that need to be documented and maintained, including where and in what manner the artifacts are to be maintained, such as:
    - Business owner approval to initiate a change.
    - Business owner prioritization of a change.
    - Test plans.
    - Test results.
    - Business owner approval to implement a change.
    - Business owner post-implementation review.

    DTMB's lack of guidance regarding documenting and maintaining artifacts resulted in the deficiencies noted in Finding #3.

b. Defining the roles and responsibilities of the:
    - Configuration management manager.
    - Business owner.
    - Developer.
    - Quality assurance testing (QAT) tester.
    - User acceptance testing* (UAT) tester.

c. Defining appropriate segregation of duties, such as:
    - Only business owners should authorize the initiation of a change.
    - Developers should not perform QAT on changes they created.
    - Business owners should authorize the implementation of a change.
    - Developers should not implement their own changes into the production environment.
    - Business owners should perform UAT.
    - Business owners should perform post-implementation review.

    DTMB's lack of guidance regarding segregation of duties resulted in the deficiencies noted in Finding #5.

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

d. Defining the monitoring and oversight activities.

   For example, the audit processes conducted by the configuration management manager and the ESOGB ensure that the configuration management process is being followed.

   DTMB's lack of guidance for monitoring and oversight activities resulted in the deficiencies noted in Finding #2.

e. Categorizing change types, such as:
   - Application.
   - Operating system*.
   - Database*.

f. Defining the tests to be performed based on change type.

g. Defining emergency change management processes to be followed.

h. Defining terminology.

DTMB developed basic enterprise guidelines; however, some were incomplete and open to interpretation. DTMB Agency Services established individual processes that did not always address the necessary COBIT guidelines.

RECOMMENDATION

We recommend that DTMB fully establish comprehensive policies, standards, and procedures for its change management process.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. Prior to the start of the audit, DTMB initiated the Material Internal Control Weakness Remediation and Accountability Program (MICWRAP) to help the State ensure that departments established and followed effective change management control processes to address enterprise risks, resolve known material and reportable IT internal control weaknesses, and establish processes and measurement to reduce and/or eliminate unknown and potential similar weaknesses. MICWRAP has assisted DTMB in establishing clear and comprehensive change management policies, standards, and procedures that align with COBIT, NIST and ITIL guidelines. On April 1, 2017, DTMB implemented the State's "Enterprise application and database, change and release transition management standard" and the State's "Enterprise application and database, change and release transition management procedure." These documents clearly identify artifacts that need to be documented

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

and maintained. DTMB has defined roles and responsibilities and outlined appropriate segregation of duties in the standard. Also, DTMB has documented monitoring and oversight activities in the Change Management Center of Excellence (CMCoE) Monitoring procedure. DTMB has implemented categorization of change type in the SMMS. DTMB has defined test types based on the type of change being performed and has documented the State's change management emergency process. Further, DTMB has defined change management terminology including roles, testing, and environments, in the standard.

FINDING #2

Monitoring controls need improvement.

DTMB did not effectively monitor its change management process to help reduce the risk that intentional or inadvertent changes would impair the proper functioning or integrity of the State's IT systems.

COBIT states that management should monitor and evaluate performance and assess compliance by setting performance criteria, measurements, and targets; audit the process; identify gaps; and recommend corrective action.

DTMB did not:

a. Establish monitoring processes for application, operating system, and database changes.

b. Assign the configuration management manager role for 8 (47%) of the 17 executive branch departments.

Configuration management manager role was not assigned for 8 (47%) of the 17 departments.

SUITE indicates that the configuration management manager is responsible for processing and tracking software change requests; ensuring that changes are recorded, reviewed, and approved; and ensuring that audits are performed to encourage compliance with change management processes.

DTMB indicated that, because of the lack of staff and resources, it was unable to assign the configuration management manager role for all 17 departments.

DTMB informed us that it did not establish comprehensive enterprise procedures directing the teams within its Agency Services to establish controls and perform monitoring. DTMB also informed us that it expected its Agency Services to monitor the change management process; however, that expectation was not clearly communicated through policies, standards, and procedures.

RECOMMENDATION

We recommend that DTMB effectively monitor its change management process to help ensure that intentional or inadvertent changes would not impair the proper functioning or integrity of the State's IT systems.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. Prior to the start of the audit, DTMB initiated MICWRAP to help the State ensure that departments established and followed effective change management control processes which include the following: DTMB has established the CMCoE and change management monitoring processes to ensure that risks are identified, policies, standards and procedures are adhered to, and corrective action taken on non-compliance. The CMCoE develops and communicates performance criteria, and

monitors and reports results to DTMB's Change Management Governance Board. CMCoE's monitoring processes are documented in the "Change management center of excellence procedure". DTMB has defined the configuration management role and documented segregation of duties requirements in the "Enterprise application and database, change and release transition management standard".

IMPLEMENTATION OF CHANGE MANAGEMENT CONTROLS

BACKGROUND

An IT application's business owner typically initiates the change management process by authorizing a needed modification. DTMB or a third-party vendor then constructs the code (such as program or source code) in a development environment before moving to the test environment. While in test, it undergoes various QAT and UAT. During UAT, the business owner tests the functionality of the change and authorizes DTMB to move it into the production environment. A request for change (RFC) ticket is created and entered into DTMB's Service Management and Monitoring System* (SMMS) by DTMB Agency Services. The change is reviewed and approved by one or more LCABs and the ECAB, if necessary, for completeness and impact on the State's IT environment. After approval, Agency Services moves the change to the production environment for implementation and the business owner conducts a post-implementation review to verify that the change met expectations.

AUDIT OBJECTIVE

To assess the effectiveness* of DTMB's efforts to implement change management controls* over the State's IT applications.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Establishment and implementation of various change management controls in accordance with DTMB policies, standards, and procedures.
- Implementation of several change management tools.
- Five reportable conditions related to lack of documentation, QAT not consistently performed, segregation of duties not always enforced, improvements needed to the authorization process, and use of SMMS not enforced (Findings #3 through #7).

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

FINDING #3

Evidence of control activities not consistently documented.

DTMB did not consistently maintain documentation of control activities performed during the change management lifecycle to help ensure that all changes to the State's IT systems were properly initiated, tested, implemented, and reviewed.

Examples of documentation required by COBIT include evidence that:

- Business owners prioritized and authorized all changes.
- Changes were tested in accordance with defined test plans, prior to implementation.
- Formal sign-off of satisfactory test results exists indicating that changes were ready to move into the next testing phase.
- Business owners approved the changes for implementation.
- Post-implementation reviews assessed the extent to which:
  - Business requirements and internal and external stakeholders' expectations have been met.
  - The system was considered usable.
  - Change management implementation and accreditation processes were performed effectively and efficiently.

We reviewed 220 judgmentally selected changes. Based on the nature of the change, some audit procedures were not applicable to all 220 changes as noted in part b. Our review disclosed that DTMB did not:

a. Maintain documentation of change initiation:

Authorization of change initiation not documented for 80 (36%) of 220 changes.

(1) 80 (36%) of the 220 changes had no evidence that business owners authorized the initiation of the change.

(2) 72 (33%) of the 220 changes had no evidence that business owners prioritized the change.

b. Maintain documentation of key testing phase artifacts, such as test plans, test results, and approvals of test results, as indicated in the following table:

Testing Phase	Number of Changes Reviewed at Each Testing Phase	Changes Without Test Plans	Changes Without Test Results	Changes Without Approval of Test Results
Development	162	116 (72%)	109 (67%)	72 (44%)
QAT	77	44 (57%)	38 (49%)	37 (48%)
UAT	171	131 (77%)	95 (56%)	45 (26%)

c. Maintain documentation that business owners approved the implementation of the change for 58 (26%) of the 220 changes.

Post-implementation review documentation not maintained 56% of the time.

d. Maintain documentation that business owners performed a post-implementation review for 123 (56%) of the 220 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 lifecycle.

DTMB Agency Services informed us that it did not maintain documentation to support all phases of the change management lifecycle because of the lack of documented enterprise guidance. Agency Services also informed us that it assumed that SUITE satisfied this requirement; however, the flexibility of the SUITE process allowed key processes to be overlooked, modified, or removed.

RECOMMENDATION

We recommend that DTMB consistently maintain documentation of control activities performed during the change management lifecycle to help ensure that all changes to the State's IT systems are properly initiated, tested, implemented, and reviewed.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. Prior to the start of the audit, DTMB initiated MICWRAP to help the State ensure that departments established and followed effective change management control processes which include the following: DTMB has established policies, standards, and procedures to ensure change management documentation is stored in a central location and kept for the life of the system plus one year. Change management documentation will be maintained in one of the State's standard source tools (e.g. Serena, TFS, JIRA, or Rational), and/or via SUITE documents. DTMB implemented these documentation guidelines as of April 1, 2017.

FINDING #4

QAT not consistently performed.

DTMB did not consistently perform QAT for 9 (53%) of the 17 executive branch departments. QAT helps ensure that changes are properly designed and coded and that they reflect business owner needs.

Performing QAT also helps ensure that coding defects are identified and corrected early in the change management process. Defects are significantly more expensive to resolve the later they are detected.

Poorly controlled changes can have a significant impact on security and reliability.

ITIL states that QAT provides a comprehensive method for ensuring change quality. Also, the Federal Information System Controls Audit Manual* (FISCAM) states that testing should be comprehensive and appropriately consider security. The extent of testing will vary depending on the type of change; however, the change should be carefully controlled and approved because relatively minor coding changes, if performed incorrectly, can have a significant impact on security and overall data reliability.

According to SUITE's Testing Process Manual, QAT is a key quality control activity that includes:

Test Type	Purpose
Integration test	Verifies that system components are integrated and working. This type of testing uncovers errors that occur in the interactions and interfaces between components.
Verification test	Verifies that a product or product component fulfills its intended purpose.
Performance test	Measures software performance of batch data, under actual and anticipated volumes, as well as on-line transaction response times verifying performance requirements, throughput, and growth capacity.
System and standards test	Verifies that functional business requirements, business processes, data flows, and other system criteria are met. Tests specific end-to-end business processes until the complete application environment mimics real world use. Verifies that federal, State, and department standards are met.
Regression test	Re-executes specific test cases to ensure that defects are fixed, to find new defects that may have been introduced, and to confirm modules are functioning properly.

DTMB informed us that, while it recognizes the value of QAT, performing QAT is not always possible because of a lack of resources. Also, DTMB acknowledged that different types of

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

changes require different types and degrees of testing; however, it had not established enterprise guidance that clearly defines the depth and breadth of testing to be performed for each change type.

RECOMMENDATIONS

We recommend that DTMB consistently perform QAT in all executive branch departments.

We also recommend that DTMB establish enterprise guidance that clearly defines the depth and breadth of testing to be performed for each change type.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendations. Prior to the start of the audit, DTMB initiated MICWRAP to help the State ensure that departments established and followed effective change management control processes which include the following: As of April 1, 2017, DTMB implemented the "Enterprise application and database, change and release transition management standard," which provides enterprise guidance on QAT and its requirements. In addition, the standard includes testing definitions based off types of changes/releases, including required tests for each phase of testing. This State standard, is based on the COBIT and NIST guidelines, and will help to ensure consistent performance of QAT activities throughout the State.

FINDING #5

Segregation of duties not always enforced.

DTMB should improve the segregation of duties throughout the change management lifecycle to reduce the risk that unintended or unauthorized changes are implemented in the State's IT environment.

COBIT states that segregation of duties should be established to ensure that individuals cannot bypass controls and to ensure the oversight of the change management process.

Our review of 220 judgmentally selected changes disclosed that DTMB did not always ensure that appropriate segregation of duties were followed. Based on the nature of the change, some audit procedures were not applicable to all 220 changes as noted below:

a. For 36 (16%) of 220 changes, DTMB, instead of the business owner, authorized the initiation of the change. The business owner should authorize the initiation of all changes.

b. For 31 (40%) of 77 changes, DTMB did not prevent developers from performing QAT on their own work:

   (1) For 2 (6%) of the 31 changes, the developers performed QAT on their own work.

   (2) For 29 (94%) of the 31 changes, DTMB did not maintain documentation to support that developers did not perform their own QAT.

c. For 53 (31%) of 171 changes, DTMB did not ensure that the business owner performed UAT testing:

   (1) For 15 (28%) of the 53 changes, DTMB, rather than the business owner, performed UAT.

   (2) For 38 (72%) of the 53 changes, DTMB did not maintain documentation to support that the business owners performed UAT.

d. For 19 (9%) of 220 changes, DTMB authorized the implementation of the change. All changes should be authorized by the business owner prior to implementing the change into production.

e. For 12 (7%) of 170 changes, DTMB did not prevent developers from implementing their own work into the production environment:

   (1) In 3 (25%) of the 12 changes, the developers implemented their own work.

   (2) In 9 (75%) of the 12 changes, DTMB did not maintain documentation to support that individuals

independent from development implemented the change into production.

f. For 8 (4%) of 220 changes, DTMB performed the post-implementation review. This review should be performed by the business owners to ensure that the change met their expectations.

Although we noted a significant number of errors related to the authorization, testing, and implementation of changes, we identified compensating controls that reduced the risk of improper actions.

DTMB informed us that it did not consistently document the segregation of roles and duties for all change management lifecycle phases because of the lack of documented enterprise guidance, funding, and resources.

RECOMMENDATION

We recommend that DTMB improve the segregation of duties throughout the change management lifecycle to reduce the risk that unintended or unauthorized changes are implemented in the State's IT environment.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. Prior to the start of the audit, DTMB initiated MICWRAP to help the State ensure that departments established and followed effective change management control processes which include the following: As of April 1, 2017, DTMB implemented the State's "Enterprise application and database, change and release transition management standard," to help ensure segregation of duties throughout the change management lifecycle. The standard requires change management release teams to ensure the following:

- *Business owner is required to initiate the change request.*
- *Business owner prioritizes and Authorizes which changes are to be included in a release.*
- *Business owner authorizes the change/release.*
- *Business owner performs/approves UAT completion results.*
- *Business owner performs validation after production implementation.*
- *DTMB management authorizes the change to be developed.*
- *Development tester, QAT tester, or UAT tester must be assigned as an authorized tester and cannot be the assigned DTMB developer.*

- *Developer cannot authorize the change/release (at any phase).*
- *Developer cannot implement the change/release into any environment higher than development.*
- *Implementer cannot implement the change/release if they developed the change/release.*
- *Database administrator cannot implement application changes/releases.*
- *Configuration manager cannot physically implement database changes/releases.*

FINDING #6

Improvements to authorization process needed.

DTMB did not consistently create and maintain listings of persons authorized to approve changes at each phase of the change management lifecycle. As a result, DTMB could not demonstrate that changes were properly authorized.

FISCAM states that policies and procedures should be in place that detail who can authorize a change. Generally, the business owners have primary responsibility for authorizing changes. The entity's configuration management plan should include requirements for defining responsibilities for each person involved in approving changes, including who should approve test results before implementation. Emergency procedures should specify who may authorize emergency changes.

DTMB provided us with its listings of the individuals who were authorized to approve the following change management lifecycle activities:

- Initiation of changes.
- Development testing results.
- QAT results.
- UAT results.
- Implementation of changes.

Our review of authorization listings disclosed:

For 12 (71%) of the 17 departments, DTMB had not created authorization listings.

a. For 12 (71%) of the 17 executive branch departments, DTMB had not created authorization listings for any phase of the change management lifecycle prior to our audit.

b. For 5 (29%) of the 17 executive branch departments, DTMB did not always maintain historical and updated authorization listings.

Although we noted a significant number of exceptions, our testing procedures did not identify that any inappropriate individuals authorized the changes, except for the segregation of duties issues noted in Finding #5.

DTMB Agency Services informed us that it was not necessary to document the authorization listings because it was familiar with the appropriate approvers.

RECOMMENDATION

We recommend that DTMB consistently create and maintain authorization listings for each phase of the change management lifecycle.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. Prior to the start of the audit, DTMB initiated MICWRAP to help the State ensure that departments established and followed effective change

management control processes which include the following: As of April 1, 2017, DTMB established the "Enterprise application and database, change and release transition management standard", to ensure that the department consistently creates and maintains authorization listings for each phase of the change management process. The standard also includes requirements for authorization list documentation and central storage requirements; maintenance requirements for authorized approver lists for each phase of the change management lifecycle; source tool requirements; authorization requirements; and SUITE document requirements.

FINDING #7

Use of SMMS should be enforced.

DTMB did not input all changes into the Service Management and Monitoring System (SMMS) to ensure that all changes were identified, authorized, and assessed for adverse impact on the State's IT environment prior to implementation.

DTMB Technical Standard 1340.00.060.04 states that the primary objective of change management is to plan, document, and approve all changes that could have an effect on IT services. Also, DTMB Technical Procedure 1340.00.060.04.03 requires that all changes be submitted into SMMS as an RFC ticket and that an RFC violation be issued for changes made without an approved RFC ticket.

DTMB Agency Services did not follow proper SMMS procedures 27% of the time.

Our review of 209 judgmentally selected changes disclosed that DTMB Agency Services did not follow proper procedures for entering changes into SMMS for 57 (27%) of the changes. Also, DTMB Data Center Operations (DCO) did not issue RFC violations for the 57 changes.

Agency Services informed us that it was unaware that all changes were required to go through the RFC process. Also, because of the decentralization of the change management process, DCO informed us that it did not have a control in place to ensure that all changes are documented in SMMS. Because DCO relies on Agency Services to self-report and enter changes into SMMS, DCO only becomes aware of a change after an RFC ticket is created in SMMS.

RECOMMENDATIONS

We recommend that DTMB input all changes into SMMS to ensure that all changes are identified, authorized, and assessed for adverse impact on the State's IT environment prior to implementation.

We also recommend that DTMB implement a control process to ensure that the change management process is followed.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendations. Prior to the start of the audit, DTMB initiated MICWRAP to help the State ensure that departments established and followed effective change management control processes which include the following: DTMB established the State's "Enterprise application and database, change and release transition management standard", and the State's "Enterprise application and database, change and release transition management procedure", to enforce the use the SMMS and require its use for all production application/database changes. DTMB Technical Procedure 1340.00.060.04.01 was a pre-existing procedure but has been updated to require that all production application/database changes and all infrastructure environments, excluding sandbox and labs, require a request for change in the SMMS. In addition, DTMB has established a

monitoring process to ensure that the SMMS request for change process and procedures are adhered to, and corrective action is taken for non-compliance to the standard. DTMB has established the CMCoE and change management monitoring processes to ensure that risks are identified, policies, standards and procedures are adhered to, and corrective action taken on non-compliance. The CMCoE develops and communicates performance criteria, monitors and reports results to DTMB's Governance Board. CMCOE's monitoring processes are documented in the "Change management center of excellence procedure".

DESCRIPTION

Change management is the process of controlling changes to the infrastructure or any aspect of IT services in a controlled and planned manner, enabling approved changes with minimal disruption to operations. Change management controls ensure that modifications to the State's IT applications are properly authorized, tested, documented, and monitored.

Various DTMB teams are involved in the State's change management process:

1. Agency Services

   - Responsible for implementing changes to the State's IT applications.
   - 7 DTMB Agency Services teams are responsible for providing IT support to the 17 executive branch departments.

2. Enterprise Service Operations Governance Board (ESOGB)

   - Defines policy and direction for LCABs and the ECAB.
   - Enforces the State's change management standards and policies.
   - Reviews and approves RFCs that impact multiple organizations.
   - Reviews and approves new LCAB requests.
   - Approves emergency RFCs that arise between the weekly ECAB meetings.
   - Comprised of representatives across DTMB's organizational environment (Network and Telecommunications Services Division, Data Center Operations, Technical Services, Design and Delivery, Client Service Center, Michigan Cyber Security, and four Agency Services representatives).

3. Data Center Operations (DCO) / Service Management Center

   - Maintains and manages SMMS.
   - Facilitates ECAB meetings and publishes ECAB meeting minutes.
   - Identifies violations of the RFC process.

4. Enterprise Change Advisory Board (ECAB)

    - Responsible for reviewing and approving RFCs that impact multiple agencies.

    - May approve an RFC on behalf of an LCAB.

    - Comprised of a representative from each LCAB.

5. Local Change Advisory Boards (LCABs)

    - Review and approve internally generated RFCs and RFCs that impact their organizations for completeness, accuracy, and impact to service.

    - During the audit period, 26 LCABs were in operation.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the program and other records related to Statewide change management 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.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2015 through February 28, 2017.

METHODOLOGY

We conducted a preliminary survey of DTMB's change management practices to formulate a basis for defining our audit objectives and scope. During our preliminary survey, we:

- Interviewed DTMB management to obtain an understanding of the processes for managing application change records and RFC tickets.
- Reviewed DTMB's SUITE process and applicable DTMB policies, standards, and procedures.
- Reviewed industry best practices.
- Analyzed RFC data stored within SMMS.

OBJECTIVE #1

To assess the sufficiency of DTMB's governance structure over change management processes related to the State's IT applications.

To accomplish this objective, we:

- Reviewed DTMB policies and procedures and compared them to industry best practices.
- Interviewed DTMB management and staff to obtain an understanding of the change management governance structure and the SUITE process.
- Interviewed DTMB management to obtain an understanding of the change management monitoring process.

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

- Observed various LCAB meetings, an ECAB meeting, and an ESOGB meeting.

OBJECTIVE #2

To assess the effectiveness of DTMB's efforts to implement change management controls over the State's IT applications.

To accomplish this objective, we:

- Judgmentally selected and reviewed 220 changes from approximately 9,300 changes recorded in the various release management* systems between October 1, 2015 and March 31, 2016.

- Judgmentally selected and reviewed 209 changes from approximately 1,300 RFCs in SMMS between October 1, 2015 and March 31, 2016.

We made our selections using a risk-based approach on each department's percentage of total changes. Because our selections were judgmental, 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.

AGENCY RESPONSES

Our audit report contains 7 findings and 9 corresponding recommendations. DTMB's preliminary response indicates that it agrees with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion at the end of our audit 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 submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services 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

change management controls	Controls that ensure that program, system, or infrastructure modifications are properly authorized, tested, documented, and monitored.
CMCoE	Change Management Center of Excellence.
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.
database	A collection of information that is organized so that it can be easily accessed, managed, and updated.
DCO	Data Center Operations.
DTMB	Department of Technology, Management, and Budget.
ECAB	Enterprise Change Advisory Board.
effectiveness	Success in achieving mission and goals.
ESOGB	Enterprise Service Operations Governance Board.
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*.
Information Technology Infrastructure Library (ITIL)	A framework, published by AXELOS, designed to standardize the selection, planning, delivery and support of IT services to a business with a goal of improving efficiency and achieving predictable service levels.
IT	information technology.
LCAB	Local Change Advisory Board.
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.
MICWRAP	Material Internal Control Weakness Remediation and Accountability Program.
mission	The main purpose of a program or an entity or the reason that the program or the entity was established.
NIST	National Institute of Standards and Technology.
operating system	The essential program in a computer that manages all the other programs and maintains disk files, runs applications, and handles devices such as the mouse and printer.
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.
QAT	quality assurance testing.
release management	A process used to manage, plan, schedule, and control a software development change through different stages and environments of the change management lifecycle.
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.
RFC	request for change.
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.

Service Management and Monitoring System (SMMS)	A DTMB application system managed by DCO in which RFCs are submitted and tracked through the various phases of the RFC process. SMMS will track the RFC from the date it was created to the date the RFC was completed and closed.
State Unified Information Technology Environment (SUITE)	The framework used by DTMB to deliver IT projects to State agencies including systems engineering, project management, procurement, and security. SUITE requires adherence to policies and procedures and creation of sound documentation.
user acceptance testing (UAT)	A process of verifying that a software solution works for the user. UAT acts as a final verification of the required business functionality and proper functioning of the system, emulating real world usage conditions.

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8060, Ext. 1650