MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

MICHIGAN ADMINISTRATIVE INFORMATION NETWORK (MAIN) SECURITY

STATE BUDGET OFFICE AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

October 2010

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

071-0594-09

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

Audit report information can be accessed at:
http://audgen.michigan.gov

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Michigan Administrative Information Network (MAIN) Security

State Budget Office and Department of Technology, Management & Budget

Report Number:
071-0594-09

Released:
October 2010

The Michigan Administrative Information Network (MAIN) is the State's automated administrative management system that supports accounting, purchasing, and other financial management activities. For fiscal year 2008-09, MAIN processed revenue and expenditure/expense transactions totaling $116.9 billion.

Audit Objective:

To assess the effectiveness of the Office of Financial Management (OFM) and the Department of Technology, Management & Budget's (DTMB's) security management controls for MAIN.

Audit Conclusion:

OFM and DTMB's security management controls for MAIN were moderately effective. We noted one material condition (Finding 1) and four reportable conditions (Findings 2 through 5).

Material Condition:

DTMB had not established, and did not ensure that the third party service organization (TPSO) established, effective controls to monitor system activity and identify security violations (Finding 1).

Reportable Conditions:

DTMB had not implemented all components of an effective mainframe security function (Finding 2).

DTMB did not ensure the completeness and effectiveness of security requirements defined in MAIN's security plan (the GSD-331) (Finding 3).

OFM and DTMB had not completed risk assessments of MAIN general and application controls and of the risks associated with using a TPSO (Finding 4).

OFM and DTMB did not fully implement the controls identified in the User Control Considerations section of the TPSO's Statement on Auditing Standards No. 70 report (SAS 70 report). In addition, OFM and DTMB did not document their assessment of internal control exceptions identified in the TPSO's SAS 70 report. (Finding 5)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:

To assess the effectiveness of DTMB's efforts to secure access to critical MAIN operating system, application, and data resources.

Audit Conclusion:

DTMB's efforts to secure access to critical MAIN operating system, application, and data resources were moderately effective. We noted one material condition (Finding 6).

Material Condition:

OFM and DTMB had not established effective access controls over MAIN operating system, application, and data resources (Finding 6).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

Our audit report contains 6 findings and 7 corresponding recommendations. DTMB did not express agreement or disagreement with any of the recommendations.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

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

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

October 14, 2010

Mr. Robert L. Emerson, State Budget Director
State Budget Office
Department of Technology, Management & Budget
and
Ms. Phyllis Mellon, Acting Director
Department of Technology, Management & Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Emerson and Ms. Mellon:

This is our report on the performance audit of Michigan Administrative Information Network (MAIN) Security, State Budget Office and Department of Technology, Management & Budget (DTMB).

This report contains our report summary; description of system and agencies; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from DTMB's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

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

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

MICHIGAN ADMINISTRATIVE INFORMATION NETWORK (MAIN) SECURITY
STATE BUDGET OFFICE
AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

Description of System and Agencies

The Michigan Administrative Information Network (MAIN) is the State's automated administrative management system that supports accounting, purchasing, and other financial management activities. For fiscal year 2008-09, MAIN processed revenue and expenditure/expense transactions totaling $116.9 billion.

MAIN was implemented on October 1, 1994. The Department of Management and Budget (DMB) created an organizational unit called DMB-MAIN to administer the system. In October 2001, Executive Order No. 2001-3 transferred the responsibility for MAIN from DMB-MAIN to the Michigan Department of Information Technology (MDIT).

Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management & Budget (DTMB), effective March 21, 2010. It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of MDIT to DTMB by a Type III transfer and abolished MDIT. In addition, it renamed the Office of the State Budget as the State Budget Office.

Since December 1, 1993, DTMB and its predecessor (DMB) have contracted with a third party service organization (TPSO) to provide technical services for MAIN, including mainframe processing, e-business environment, Financial Electronic Data Interchange (FEDI) network operations, application development services, and business recovery services. DTMB's current contract with the TPSO expires on December 31, 2011. In fiscal years 2007-08 and 2008-09, DTMB paid the contractor $5.6 million and $6.0 million, respectively, for MAIN related services.

Office of Financial Management (OFM), State Budget Office, Department of Technology, Management & Budget (DTMB)

OFM has overall responsibility for the State's accounting and payroll functions and related systems. OFM is responsible for performing central accounting and payroll control activities; developing and issuing Statewide accounting policies; maintaining the central vendor/payee file; advising State agencies on the application of generally accepted accounting principles and the use of the State's accounting system; monitoring compliance by agencies with State accounting policies; and preparing periodic financial reports, including the *State of Michigan Comprehensive Annual Financial Report*.

Bureau of Agency Services, Department of Technology, Management & Budget (DTMB)

DTMB's Bureau of Agency Services provides software development and maintenance, project management, and security* administration for MAIN.

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

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of Michigan Administrative Information Network (MAIN) Security, State Budget Office and Department of Technology, Management & Budget (DTMB), had the following objectives:

1. To assess the effectiveness* of the Office of Financial Management (OFM) and DTMB's security management controls for MAIN.

2. To assess the effectiveness of DTMB's efforts to secure access to critical MAIN operating system*, application, and data resources.

Audit Scope

Our audit scope was to examine the information processing and other records related to Michigan Administrative Information Network security. 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 procedures, conducted from June through October 2009, generally covered the period August 2008 through October 2009.

Audit Methodology

The criteria used in the audit included control techniques and suggested audit procedures from the U.S. Government Accountability Office's (GAO's) *Federal Information System Controls Audit Manual,* control objectives and audit guidelines outlined in the Control Objectives for Information and Related Technology* (COBIT) issued by the IT Governance Institute, and other information security and industry best practices.

To establish our audit objectives, we conducted a preliminary review of general controls* over MAIN. In addition, we obtained an understanding of the MAIN system

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

architecture. We also performed a preliminary analysis of data obtained from Resource Access Control Facility (RACF) security reports.

To accomplish our first objective, we reviewed and assessed OFM and DTMB's security related policies and procedures. In addition, we reviewed security requirements in the State's contract with the third party service organization (TPSO). We also assessed the effectiveness of security management control requirements in the GSD-331*, which is the security agreement between the State of Michigan and the TPSO, and assessed OFM and DTMB's processes to ensure that security management controls at the TPSO were documented, placed in operation, and monitored. Finally, we reviewed and assessed the effectiveness of MAIN's security administration function.

To accomplish our second objective, we reviewed and tested the configuration of RACF. In addition, we reviewed the completeness and effectiveness of access requirements in the GSD-331. We also evaluated the appropriateness of access granted to selected MAIN operating system, application, and data resources.

This report summarizes security and access control* weaknesses in MAIN. It does not contain detailed examples of the security and access control weaknesses identified because of their sensitive nature. During the course of the audit, we provided OFM and DTMB management with detailed examples of the security and access control weaknesses identified during our fieldwork.

When selecting activities or programs for audit, we use an approach based on assessment of risk and opportunity for improvement. Accordingly, we focus our audit efforts on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. Our limited audit resources are used, by design, to identify where and how improvements can be made. Consequently, we prepare our performance audit reports on an exception basis.

Agency Responses

Our audit report contains 6 findings and 7 corresponding recommendations. DTMB did not express agreement or disagreement with any of the recommendations.

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

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion subsequent to 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 DTMB to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF SECURITY MANAGEMENT CONTROLS

COMMENT

Background: Effective security management controls provide a foundation for an organization's management to obtain reasonable assurance that its applications are effectively secured. Security management controls provide a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's application controls*. Without effective security management controls, there is an increased risk that an organization's management, information technology* (IT) staff, application owners, and users will not implement appropriate and adequate information security over the application.

When an organization utilizes a third party service organization (TPSO) for purposes such as hosting financial accounting systems, the TPSO's controls become a key component in the organization's internal control*. However, an organization's management is ultimately responsible for the achievement of the organization's internal control objectives.

Audit Objective: To assess the effectiveness of the Office of Financial Management (OFM) and the Department of Technology, Management & Budget's (DTMB's) security management controls for the Michigan Administrative Information Network (MAIN).

Audit Conclusion: OFM and DTMB's security management controls for MAIN were moderately effective. Our assessment disclosed one material condition*. DTMB had not established, and did not ensure that the TPSO established, effective controls to monitor system activity and identify security violations (Finding 1).

Our assessment also disclosed four reportable conditions* related to mainframe security function, security requirements, risk assessments*, and effectiveness of the TPSO's controls (Findings 2 through 5).

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

FINDING

1. Monitoring Controls

DTMB had not established, and did not ensure that the TPSO established, effective controls to monitor system activity and identify security violations. As a result, DTMB and the TPSO cannot ensure that users perform only the activities for which they have been explicitly authorized.

According to the Control Objectives for Information and Related Technology (COBIT), staff experienced in security testing and monitoring should test and monitor the IT security implementation in a proactive way. For example, the logging and monitoring of security related events will enable the early prevention or detection and subsequent timely reporting of unusual or abnormal activities. In addition, security administrators should routinely validate that security related system parameters are defined correctly and are in compliance with the information security baseline. Our review disclosed:

a. DTMB and the TPSO did not routinely review sensitive system access. MAIN's security plan, the GSD-331, required the logging of system access impacting security. However, neither DTMB nor the TPSO periodically reviewed the logs.

b. DTMB did not ensure that the TPSO routinely reviewed the activities of privileged users, such as system administrators, computer operators, and database administrators. In addition, neither DTMB nor the TPSO routinely monitored the appropriateness of users' actions performed using certain systemwide privileged authority. The TPSO informed us that, although privileged users' activities may be logged, the logs are not reviewed unless the TPSO becomes aware of a problem.

c. DTMB had not documented procedures to ensure the timely identification and follow-up of potential security violations. Although MAIN's security administrator informed us that he monitored daily and weekly logs for access violations, DTMB had not documented the types of events requiring follow-up, the frequency of review, and the expected actions.

d. DTMB could improve its oversight of the TPSO's monitoring activities by independently validating that the Resource Access Control Facility (RACF)

and other security parameters are configured in agreement with the GSD-331. The TPSO utilizes a proprietary scanning tool to ensure that RACF and other system parameters agree with the GSD-331. DTMB informed us that it does not have the means to validate that the TPSO's scanning tool has been properly configured to test for differences in the configuration settings. Instead, DTMB relies upon the TPSO to identify and report configuration discrepancies. Independently validating RACF and other security parameters would help DTMB ensure that the TPSO secures MAIN in accordance with the agreed-upon security settings.

RECOMMENDATION

We recommend that DTMB establish, and ensure that the TPSO establishes, effective controls to monitor system activity and identify security violations.

AGENCY PRELIMINARY RESPONSE

DTMB did not express agreement or disagreement with this recommendation. DTMB informed us that it believes that the controls over MAIN monitoring are effective but agrees that they could be improved. DTMB, in conjunction with OFM, is currently evaluating the auditor's monitoring control recommendation for MAIN and will comply with those parts of the finding that can be implemented in a cost-effective manner and pose no negative impact to the existing operations.

FINDING

2. Mainframe Security Function

DTMB had not implemented all components of an effective mainframe security function. As a result, DTMB cannot ensure that appropriate information security controls have been implemented to protect the State's financial data and to provide proper oversight of the TPSO.

Our review of the mainframe security function for MAIN disclosed:

a. MAIN's security administrators did not perform important security-related activities. For example, the security administrators did not review security plans, facilitate risk assessments, monitor privileged access*, remediate

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

control weaknesses, and provide oversight of TPSO. The security administrators did not perform these activities because DTMB had not assigned responsibility for the activities in the security administrators' position descriptions. In addition, the security administrators' position descriptions did not specify the necessary knowledge, skills, and abilities needed to effectively perform security administrator duties.

COBIT states that management should ensure that position descriptions define the skills, experience, responsibilities, and authority for IT personnel.

b. DTMB did not ensure proper segregation of duties* in its assignment of security administration responsibilities. DTMB informed us that the responsibility for MAIN security was shared between two individuals. DTMB assigned the responsibility of monitoring access violations to an individual who had the conflicting responsibility of user identification (ID) administration. In addition, the other individual whom DTMB designated as a security administrator had conflicting responsibilities as manager over MAIN system development and maintenance.

   COBIT states that management should implement a division of roles and responsibilities to prevent a single individual from circumventing a critical control process. Therefore, DTMB should maintain a segregation of duties between the system development and maintenance, user ID administration, and security administration functions.

c. DTMB could improve security administrator training. The security administrators informed us that they had not received formal security training specific to MAIN's operating system platform.

   MAIN resides on a highly complex operating system platform. There are many interrelated components of the operating system that must be securely configured, including the mainframe's security system, file system, database management system, data communication systems, transaction management system, job scheduling system, change control systems, and tape management system. Without a comprehensive understanding of the operating system platform, the security administrators will not be able to

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

effectively perform their security responsibilities, such as reviewing and approving the GSD-331, performing risk assessments, and overseeing the TPSO.

COBIT states that management should provide personnel with the appropriate education and training to maintain adequate competence and, where appropriate, encourage skills certification.

d. MAIN's security administrators were not granted auditor privileges. As a result, the security administrators did not have the ability to independently run auditing reports or to control system logging options.

COBIT states that management should provide appropriate resources to ensure that personnel can carry out their security responsibilities.

RECOMMENDATION

We recommend that DTMB implement all components of an effective mainframe security function.

AGENCY PRELIMINARY RESPONSE

DTMB did not express agreement or disagreement with this recommendation. DTMB informed us that it believes that the controls over the MAIN mainframe security function are effective but agrees that they could be improved.

DTMB informed us that it is already addressing two of the four parts of the finding. DTMB stated that the segregation of duties weakness has been remediated and both security administrators will be provided with the necessary level of privileges to adequately perform their roles.

DTMB also informed us that DTMB, in conjunction with OFM, is currently considering the remaining two parts of the finding for the MAIN mainframe security function and will comply with the corresponding recommendation where solutions can be implemented in a cost-effective manner and pose no negative impact to the existing operations.

FINDING

3. Security Requirements

DTMB did not ensure the completeness and effectiveness of security requirements defined in the GSD-331. Therefore, DTMB cannot ensure that RACF and other system parameters have been properly configured to protect critical operating system, application, and data resources.

In the GSD-331, DTMB and the TPSO defined security practices and established their respective roles and responsibilities. In addition, the GSD-331 implementation guide defined operating system and application parameters specific to MAIN. DTMB informed us that some of the configuration settings were last reviewed in 2002 when the TPSO contract was renegotiated. DTMB acknowledged that the configuration settings may not be in alignment with current security standards.

DTMB had not effectively assessed the security requirements in the GSD-331 because it had not adopted a technical standard for securing RACF and other operating system configuration parameters. Although DTMB has adopted COBIT for its IT governance and control standard, COBIT does not provide the detailed configuration guidance necessary to ensure that the security requirements in the GSD-331 align with DTMB's risk and security objectives.

Our review disclosed:

a. DTMB did not ensure that the GSD-331 included configuration settings for all high-risk system parameters. High-risk system parameters are configuration settings that impact the operating system's security and performance. As a result, DTMB and the TPSO had not configured certain system parameters to prevent users and programs from bypassing RACF security or obtaining elevated privileges.

b. DTMB did not ensure that the GSD-331's configuration settings promoted and enforced strong security. For example:

   (1) DTMB did not ensure that the TPSO configured RACF to enforce strong password policies for password composition, aging, and history. Forty-eight user accounts were configured to require more frequent

password changes. However, the GSD-331 did not specify which types of user accounts required more frequent password changes.

(2) DTMB did not ensure that the TPSO configured RACF to revoke an inactive user's account after an appropriate length of time. DTMB informed us that because data sets* and other resources are assigned to an individual's user ID, rather than a group, it cannot revoke an inactive user's account until the resources are reassigned.

(3) DTMB did not ensure that the TPSO configured RACF to log alter and update activity on the system logs. Because users attempting to conceal inappropriate or unauthorized activity may try to delete or destroy information from the system logs, all alter and update activity should be logged and monitored.

(4) DTMB could strengthen the security banner on the MAIN application login screen by requesting that the TPSO modify the banner to refer to the penalties for unauthorized access. National Institute of Standards and Technology special publication 800-53 recommends that security banners explicitly state that unauthorized use is prohibited and refer to applicable criminal and civil penalties for intentional unauthorized access.

c. DTMB did not document its assessment of deviations from the TPSO's security recommendations. In the GSD-331, the TPSO identified configuration settings that it believed posed potential security risks. DTMB approved and accepted responsibility for the deviations without documenting the basis for its decision or determining the need for compensating controls.

RECOMMENDATION

We recommend that DTMB ensure the completeness and effectiveness of security requirements defined in the GSD-331.

AGENCY PRELIMINARY RESPONSE

DTMB did not express agreement or disagreement with this recommendation. DTMB informed us that it believes that the controls over the MAIN system security

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

requirements are effective but agrees that they could be improved. DTMB informed us that it has already reviewed most of the recommended security requirements and implemented changes in compliance with the audit recommendation wherever those changes were cost effective and deemed to have no negative impact on existing operations. DTMB, in conjunction with OFM, will consider the remaining parts of the security requirement finding and will comply with those that can be implemented in a cost-effective manner.

FINDING

4. Risk Assessments

OFM and DTMB had not completed risk assessments of MAIN general and application controls and of the risks associated with using a TPSO. Without risk assessments, OFM and DTMB cannot efficiently direct their limited resources to implementing controls that address the greatest threats to the confidentiality, integrity, and availability of the State's financial information.

OFM and DTMB identified, in the biennial internal control evaluation (BICE) for MAIN, some general and application controls that, if operating effectively, would reduce MAIN's exposure to certain risks. However, the BICE excluded many key components of a risk assessment, such as system characterization, threat identification, vulnerability identification, likelihood determination, impact analysis, risk determination, and control recommendations. As a result, OFM and DTMB cannot ensure that the IT controls identified in the BICE sufficiently addressed and mitigated all significant risks.

According to COBIT, management should periodically assess threats and vulnerabilities that could have a potential negative impact on business operations. In addition, COBIT states that the risk assessment process should determine the likelihood and impact of all identified risks and that management should develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis.

RECOMMENDATION

We recommend that OFM and DTMB complete risk assessments of MAIN general and application controls and of the risks associated with using a TPSO.

AGENCY PRELIMINARY RESPONSE

DTMB did not express agreement or disagreement with this recommendation. OFM and DTMB informed us that they believe that the controls over MAIN risk assessments are effective but agree that they could be improved. OFM and DTMB also informed us that they are planning a complete risk assessment at the State of Michigan and the TPSO for MAIN pending the availability of funding and resources.

FINDING

5. Effectiveness of the TPSO's Controls

OFM and DTMB did not fully implement the controls identified in the User Control Considerations section of the TPSO's Statement on Auditing Standards No. 70 report (SAS 70 report*). In addition, OFM and DTMB did not document their assessment of internal control exceptions identified in the TPSO's SAS 70 report. As a result, internal control weaknesses may exist that impair the effectiveness of MAIN's internal control.

A SAS 70 report describes controls at the TPSO that may be relevant to MAIN's internal control. For the period December 1, 2007 through November 30, 2008, the SAS 70 report concluded that the TPSO's controls were suitably designed, had been placed in operation, and would achieve the TPSO's control objectives if the user organization (the State of Michigan) implemented the controls described in the User Control Considerations section of the SAS 70 report. However, our review disclosed:

a. OFM and DTMB could not provide documentation such as policies and procedures or other evidence that it had implemented 10 of 20 user controls. For example, OFM and DTMB had not established procedures to ensure the timely revocation of access, to ensure that access privileges meet industry best standards, and to ensure that the operating system and applications are protected from unprivileged users. Incomplete implementation of user controls increases the likelihood that the internal control at the TPSO will not be effective.

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

b. OFM and DTMB did not document the impact on MAIN of exceptions identified in the TPSO's SAS 70 report and did not include any relevant exceptions in their BICE. As a result, OFM and DTMB cannot ensure that the relevant internal control exceptions at the TPSO were properly reported and remediated. The State of Michigan Financial Management Guide requires the manager responsible for oversight of the TPSO to document the method for ensuring the effectiveness of controls and the results of control assessments. In addition, the Guide requires the agencies' internal control officers to consider the impact of the TPSO in the agencies' BICE.

RECOMMENDATIONS

We recommend that OFM and DTMB fully implement the controls identified in the User Control Considerations section of the TPSO's SAS 70 report.

We also recommend that OFM and DTMB document their assessment of internal control exceptions identified in the TPSO's SAS 70 report.

AGENCY PRELIMINARY RESPONSE

DTMB did not express agreement or disagreement with these recommendations. OFM and DTMB informed us that they believe that the TPSO controls over MAIN are effective but agree that they could be improved. OFM and DTMB also informed us that they are currently evaluating the auditor's TPSO control recommendations for MAIN and will comply with those parts of the finding that can be implemented in a cost-effective manner and pose no negative impact to the existing operations.

EFFECTIVENESS OF DTMB'S EFFORTS TO SECURE ACCESS

COMMENT

Background: Access controls restrict access or detect inappropriate access to computer resources, thereby protecting the resources from unauthorized modification, loss, and disclosure. Logical access controls require users to authenticate themselves, through the use of secret passwords or other identifiers, and limit the files and other resources that users can access and actions that they can execute.

Audit Objective: To assess the effectiveness of DTMB's efforts to secure access to critical MAIN operating system, application, and data resources.

Audit Conclusion: DTMB's efforts to secure access to critical MAIN operating system, application, and data resources were moderately effective. Our assessment disclosed one material condition. OFM and DTMB had not established effective access controls over MAIN operating system, application, and data resources (Finding 6).

FINDING

6. Access to Resources

OFM and DTMB had not established effective access controls over MAIN operating system, application, and data resources. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, could read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users could intentionally or unintentionally read, add, delete, modify, or copy data or execute changes that are outside their span of authority.

According to COBIT, access controls should include policies and procedures for requesting, approving, and periodically reviewing user access and restricting access to sensitive system resources. Our review disclosed:

a. DTMB did not ensure that privileged access rights were granted to individuals based on the principle of least privilege* and promoted a proper segregation of duties. Privileged access rights enable a user to bypass established controls. DTMB Administrative Guide policy 1335 requires agencies to implement access control policies and procedures to promote least privilege, segregation of duties, and the granting of access on a need-to-know basis. Our review of privileged access rights disclosed:

   (1) DTMB did not ensure that the TPSO restricted the systemwide security administration privilege to only those individuals responsible for managing user accounts and assigning access to system resources. The TPSO granted 24 of 43 TPSO employees, who did not appear to be responsible

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

for security administration, the systemwide security administration privilege.

(2) DTMB did not ensure that the TPSO restricted the systemwide operations support privilege to only those individuals who were responsible for storage maintenance functions. This privilege allowed individuals to manage all mainframe disk and tape files. It provided full access to files, such as read, copy, add, delete, and modify capabilities. The TPSO granted 17 of 37 TPSO employees, who did not appear to be responsible for system storage maintenance, the systemwide operations support privilege.

(3) DTMB did not ensure that the TPSO restricted the systemwide auditor privilege to those individuals who were responsible for systemwide auditing of security settings. The TPSO granted the auditor privilege to 36 TPSO employees who were not responsible for systemwide auditing of RACF security and who appeared to have conflicting job responsibilities, such as RACF, database, and performance support.

(4) DTMB did not ensure that the TPSO restricted its employees from having multiple incompatible access rights. The TPSO granted 21 TPSO employees who were on the production environment and 22 TPSO employees who were on the development environment both security administration and operations support privileges. Employees with incompatible functions such as these could inadvertently or intentionally grant themselves or others the ability to copy, add, delete, and modify production programs and data without authorization.

In addition, the TPSO granted 9 TPSO employees who were on the production environment and 8 TPSO employees who were on the development environment both security administration and auditor privileges. Because employees who were granted the auditor privilege could turn off system logs used for monitoring, the auditor privilege should have been granted to individuals other than those responsible for managing users and granting access to system resources.

(5) DTMB should limit the scheduling software's access to production resources. At the time MAIN was implemented, the scheduling software

was granted the operations support privilege. Because DTMB and the TPSO run all jobs using the scheduling software's user ID, it is possible for individuals submitting jobs to inappropriately add, delete, or modify financial data.

b. DTMB did not ensure security over operating system data sets and utility programs. DTMB security, development, and technical support employees and TPSO employees who were not directly responsible for supporting the operating system or utility programs had the ability to update or delete files containing system parameters and other codes that control how the system operates and impact MAIN application security. Inappropriate access to operating system data sets could adversely impact the integrity of the operating system and allow unauthorized changes to the application and data.

c. OFM and DTMB did not ensure security over production data sets. DTMB security and technical support employees, OFM application support employees, and TPSO employees had the ability to update or delete production data sets containing application related resources, such as application source and object code, interface files, job control language, reports, and data. Users with the ability to update and delete production data sets could bypass application controls designed to protect the integrity of the MAIN application and data.

d. DTMB did not ensure that the TPSO effectively secured database access. The TPSO granted its employees privileged access that should be restricted to those individuals responsible for administering the database. For example, employees with privileged access have the ability to start and stop the database, create new objects, grant access, and make unauthorized changes to data.

e. DTMB did not ensure that access request forms were retained for all active user IDs. DTMB requires an access request form for each unique user ID. We tested a selection of 36 user IDs with Time Sharing Option* access to MAIN. DTMB could not provide an access request form for 7 (19%) of 36 user IDs and the TPSO could not provide documentation for 13 (36%) of 36 user

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

IDs requested. In addition, the TPSO's documentation for 3 (18%) of 16 user IDs did not contain a documented approval for access.

The TPSO informed us that its access control process does not require it to retain access documentation after two years. However, DTMB's records retention schedule requires DTMB to retain MAIN security access records for five years after the employees' need for access is no longer required.

f. DTMB did not perform an annual revalidation of employees' business need for access to MAIN. In addition, DTMB did not ensure that the TPSO had an effective revalidation process. According to the GSD-331, the State of Michigan and the TPSO are each responsible for performing an annual revalidation to certify the continued need for their employees' access. We determined that the TPSO's revalidation process does not require managers to submit positive assurance of a need for continued access. During our review of access to resources, we identified 25 user IDs for which the TPSO indicated that the individual or account no longer required access to the resource. Obtaining positive assurance would provide a more effective control.

g. OFM and DTMB had not fully established policies and procedures to manage technical support and other privileged users' access and did not ensure that the TPSO established similar policies. DTMB Administrative Guide policy 1335 states that agencies should establish formal policies and procedures to control access to State resources. In addition, COBIT states that organizations should require their contractors to comply with the organizations' policies and procedures. In section 5.0.3 of the contract to provide MAIN services, the TPSO indicated that its security practices will meet or exceed the State's requirements.

RECOMMENDATION

We recommend that OFM and DTMB establish effective access controls over MAIN operating system, application, and data resources.

AGENCY PRELIMINARY RESPONSE

DTMB did not express agreement or disagreement with this recommendation. OFM and DTMB informed us that they believe that the controls over MAIN system access are effective but agree that they could be improved. OFM and DTMB also informed us that they have remediated some of the access control weaknesses. In addition, OFM and DTMB are analyzing the impact of remediating the remaining parts of the finding and plan to implement those that are cost effective and pose no negative impact on existing operations.

GLOSSARY

Glossary of Acronyms and Terms

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
application controls	Controls that are directly related to individual computer applications. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.
BICE	biennial internal control evaluation.
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 information technology.
data set	IBM mainframe term for a computer file.
Department of Technology, Management & Budget (DTMB)	Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management & Budget (DTMB), effective March 21, 2010. It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of the Michigan Department of Information Technology (MDIT) to DTMB by a Type III transfer and abolished MDIT. In addition, it renamed the Office of the State Budget as the State Budget Office.
DMB	Department of Management and Budget.
effectiveness	Success in achieving mission and goals.
general controls	The structure, policies, and procedures that apply to an entity's overall computer operations. These controls include

	an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.
GSD-331	The security agreement between the State of Michigan and the TPSO. The GSD-331 serves as MAIN's security plan.
ID	identification.
information technology (IT)	Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources.
internal control	The organization, policies, and procedures adopted by agency management and other personnel to provide reasonable assurance that operations, including the use of agency resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition.
MAIN	Michigan Administrative Information Network.
material condition	A reportable condition that 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.
MDIT	Michigan Department of Information Technology.
OFM	Office of Financial Management.

operating system	The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve program operations, to facilitate decision making by parties responsible for overseeing or initiating corrective action, and to improve public accountability.
principle of least privilege	A basic principle in information security that holds that entities (people, processes, and devices) should be assigned the fewest privileges consistent with their assigned duties and functions.
privileged access	Extensive system access capabilities.
RACF	Resource Access Control Facility.
reportable condition	A matter that, in the auditor's judgment, 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 objectives of the audit; 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.
risk assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security

	controls that would mitigate this impact. Risk assessment is a part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
SAS 70 report	Statement on Auditing Standards No. 70 report. SAS No. 70 provides guidance for independent auditors who issue reports on the processing of transactions by a service organization for use by other auditors. There are two types of SAS 70 reports. A "report on controls placed in operation" contains a description of the service organization's controls that may be relevant to a user of the service organization's internal control. A "report on controls placed in operation and tests of operating effectiveness" states whether controls were suitably designed to achieve specified control objectives, whether they had been placed in operation as of a specific date, and whether the controls that were tested were operating with sufficient effectiveness.
security	Safeguarding an organization'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.
Time Sharing Option	Software that provides interactive communications for IBM's MVS (Multiple Virtual Storage) operating system. It allows a user or programmer to launch an application from a terminal and interactively work with it.
TPSO	third party service organization.

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL