Office of the Auditor General
Performance Audit Report

Statewide Oracle Database Controls

Department of Technology, Management, and Budget

March 2015

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

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 Oracle Database Controls

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0565-14

Released:
March 2015

The State maintains approximately 500 Oracle databases that are used for transaction processing and reporting by the State's various information technology systems. DTMB's Agency Services includes database administrator (DBA) teams that manage State agencies' Oracle databases. The State's Oracle database security and access controls are the responsibility of the DBA teams in conjunction with the data owners at the various State agencies.

Audit Objective	**Conclusion**
Objective 1: To assess the effectiveness of DTMB's efforts to implement security and access controls over the State's Oracle databases.	Moderately effective

Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
DTMB did not fully establish and implement effective security configurations for the State's Oracle databases. Potentially vulnerable security configurations existed on the databases reviewed that may hinder management's ability to prevent or detect inappropriate access to or modification of the State's data (Finding 1).	X		Agrees
DTMB, in conjunction with State agencies, did not fully establish and implement effective user access controls over the State's Oracle databases. Weaknesses were present in the user access controls that could result in inappropriate access to or modification of the State's data (Finding 2).		X	Agrees

Audit Objective	Conclusion
Objective 2: To assess the effectiveness of DTMB's efforts to establish an effective governance structure over the State's Oracle database environment.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not establish a formal training program or take other steps to ensure that all DBAs managing the State's Oracle databases received sufficient training. A training program would help ensure that DBAs have the knowledge and skills to effectively manage a secure Oracle database environment (Finding 3).	X		Agrees
DTMB did not fully establish policies and procedures for the security of the State's Oracle databases. As a result, DTMB cannot ensure that Oracle databases were securely configured to protect the confidentiality and integrity of critical data stored within the databases. Also, DTMB cannot ensure that audit logs capture the critical information necessary to detect unauthorized activity within the databases (Finding 4).		X	Agrees
DTMB should consider implementing a real-time system to manage its inventory of Oracle database software licenses. Inaccuracies existed because of the current manual process, which limited DTMB's ability to make inventory management decisions (Finding 5).		X	Agrees

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

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 • http://audgen.michigan.gov

March 27, 2015

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 Oracle Database Controls, Department of Technology, Management, and Budget.

We organized the background, findings, and recommendations 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 ORACLE DATABASE CONTROLS

This Page Left Intentionally Blank

BACKGROUND, FINDINGS, AND RECOMMENDATIONS

IMPLEMENTING SECURITY AND ACCESS CONTROLS

BACKGROUND

Security* and access controls* limit or detect inappropriate access, which is important to ensure the availability*, confidentiality*, and integrity* of data. Poor database management system* (DBMS) security not only compromises the database* but may also compromise the operating system* and other trusted network systems. The State's Oracle database security and access controls are the responsibility of the database administrator* (DBA) teams in conjunction with the data owners* at the various State agencies.

AUDIT OBJECTIVE

To assess the effectiveness* of the Department of Technology, Management, and Budget's (DTMB's) efforts to implement security and access controls over the State's Oracle databases.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Establishment and implementation of some security configurations* and access controls in accordance with State policy and best practices.

- Material condition* related to database security configurations and reportable condition* related to user access controls.

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

FINDING #1

More comprehensive security configurations are vital to protecting vulnerable Oracle databases.

DTMB did not fully establish and implement effective security configurations for the State's Oracle databases to help prevent or detect inappropriate access to or modification of the State's data.

According to ISO/IEC 27002:2005*, a well-secured database provides a protected environment to maintain the integrity and confidentiality of data. Appropriate security controls include using individual user accounts and passwords, monitoring to ensure that users are performing only the activities that they are explicitly authorized to perform, and using audit logs to record and monitor significant events.

We assessed the security configurations for 12 of the State's Oracle databases, including 7 production databases and 5 corresponding nonproduction databases, and noted:

a. Potentially vulnerable security configurations on the State's Oracle databases.

   Because of the confidentiality of these configurations, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB management.

b. Unclear communication of security requirements and lack of monitoring of security settings and databases managed by third party vendors.

   Security requirements not clearly communicated to vendors managing some State databases.

   Two (29%) of the 7 production databases and 2 (40%) of the 5 corresponding nonproduction databases in our review were managed by third party vendors. DTMB did not communicate all security requirements defined in DTMB policies for these 4 (100%) vendor-managed databases as required in the third party vendor contracts. As a result, third party vendors did not implement DTMB policies and procedures regarding database security. Securing Oracle databases is essential for ensuring the integrity and confidentiality of the State's data.

DTMB informed us that Oracle-specific configuration standards had not been established until June 2014 and that DTMB had not fully implemented those standards at the time of our review. As noted in Findings #3 and #4, a formal training program for DBAs had not been established and a minimum baseline configuration* and minimum audit log requirements for the State's Oracle databases had not been established and may have caused the security weaknesses noted in this finding.

RECOMMENDATION

We recommend that DTMB fully establish and implement effective security configurations for the State's Oracle databases.

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

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will implement more comprehensive security configurations to protect databases.

Realizing the importance of comprehensive Oracle database security standards, DTMB established the cross-agency Database Standards Committee in June 2013. The Committee developed and published its first set of database security standards (1340.00.15) and Oracle database security procedures (1340.00.15) for the State of Michigan databases in June 2014. The Committee will continue its work toward incorporating best practices around Oracle database security in the revised standards and better communicate and enforce the standards across the enterprise.

As part of the comprehensive enterprise database security initiative, DTMB also established a new Database Security Program in June 2013 for assessing and implementing various Oracle database software technologies for database encryption, data masking, audit, firewalls, and access controls. As its first priority, the Program successfully implemented full database encryption (including Oracle encryption) at rest and in transit by June 2014 across the enterprise.

The Program will continue its progress with implementing various security measures and assisting with enforcement of more comprehensive security configurations across all State Oracle databases. To better address appropriate methods for data protection and security based on the data classification and sensitivity, DTMB (Michigan Cyber Security), in collaboration with State agency security officers, created and published the new Data Classification Standard (1340.00.14) in June 2014. The new Data Classification framework will assist DTMB's DBAs in better determining appropriate security configurations for maintained and supported databases across the enterprise.

FINDING #2

Improvements are needed to database user access controls.

DTMB, in conjunction with State agencies, did not fully establish and implement effective user access controls over the State's Oracle databases to help prevent or detect inappropriate access to or modification of the State's data.

DTMB Administrative Guide policy 1335 requires the establishment of a process for controlling and documenting the allocation of user access rights based on current job responsibilities. Also, policies should be established to allow access to be managed, controlled, and periodically reviewed to ensure that user access is based on the principle of least privilege*. In addition, DTMB technical standard 1335.00.03 requires system owners to identify authorized users and specify access privileges, deactivate accounts of users terminated or transferred, and review accounts every 120 days.

We reviewed user access controls for 12 of the State's Oracle databases, including 7 production databases and 5 corresponding nonproduction databases, and noted:

a. Ineffective processes for promptly disabling user access upon the user changing positions or ending employment.

Active user accounts existed for persons no longer requiring access.

Five (42%) of the 12 databases reviewed had active user accounts for persons who no longer required access. As a result, users could gain inappropriate access to the data.

b. Ineffective processes for granting database access rights based on a user's job responsibilities.

Specifically:

User access not limited to principle of least privilege.

(1) User access was not granted based on the principle of least privilege. DTMB inappropriately granted high-risk access privileges to database accounts in 8 (67%) of the 12 databases reviewed. These users had the ability to inappropriately perform tasks such as creating or manipulating tables or viewing sensitive data within the database. Also, developers had the ability to make updates to 2 (25%) of these 8 databases (a production database and the corresponding nonproduction database). This ability increases the risk of unauthorized and untested changes to data in the production environment.

(2) Compensating controls did not exist in any of the 12 Oracle databases we reviewed to help establish accountability when users had access to shared accounts. In 10 (83%) of those databases, the accounts being shared had high-risk access privileges.

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

(3) Documentation of the authorization of user access rights did not ensure that only appropriate individuals had access to the database and that their levels of access were appropriate.

We judgmentally selected users from all 12 databases and noted:

Control Weakness	Number (and Percent) of Systems
Authorization forms:	
• Were not required.	4 (33%) of 12
• Were not always documented.	6 (75%) of 8
• Did not require data owner and/or data custodian* approval.	4 (50%) of 8
• Did not document the level of access actually granted to the user.	3 (38%) of 8

c. Inappropriate segregation of duties* for databases managed by third party vendor.

DTMB did not ensure that the third party vendor managing State databases implemented appropriate segregation of duties in 1 (50%) of 2 vendor managed production databases and the corresponding nonproduction database. The project manager for the system also served as the direct manager of the developers and as the backup DBA and performed development activities. DTMB technical standard 1340.00.15 states that segregation of duties must be established to ensure data integrity. According to the U.S. Government Accountability Office's (GAO's) Federal Information System Controls Audit Manual* (FISCAM), the following functions should be performed by different groups: information security, system design, application programming, change management, data security, database administration, and configuration management*.

d. A lack of user access reviews for many databases.

Periodic user access reviews did not occur for 10 (83%) of the 12 databases to ensure that privileges granted to each user were appropriate for the user's job responsibilities.

e. Potential vulnerabilities* because of ineffective or incomplete user access controls on the State's Oracle databases.

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

Because of the confidentiality of database controls, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB management.

User access controls were not fully established and implemented because DTMB management did not follow policies and procedures governing the granting, removal, and periodic review of users' access rights.

RECOMMENDATION

We recommend that DTMB, in conjunction with State agencies, fully establish and implement effective user access controls over the State's Oracle databases.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will implement needed improvements to database user access controls. DTMB will enforce the existing Database Security Standard 1340.00.15 in all agency databases. In addition, the Database Security Program Office will maintain records of controls being properly managed on all database security standards. DTMB will ensure that internal reviews occur frequently and randomly on each agency's databases to ensure compliance. DTMB's Database Security Program Office will assign a DBA security specialist to work with each agency to assist in training DBAs on how to properly secure their databases following the 1340.00.15 standard and other best practices available.

ESTABLISHING EFFECTIVE GOVERNANCE STRUCTURE

BACKGROUND

DTMB's Agency Services includes DBA teams that manage State agencies' Oracle databases. DBA teams may manage more than one database. DBA team managers are responsible for hiring and training the DBAs on their teams. As part of the State's Enterprise Database Security Project, DTMB established in June 2013 the State of Michigan Database Standards Committee, which is developing policies and procedures for configuring and securing the State's databases. In June 2014, DTMB issued policies and procedures for securely configuring Oracle databases.

AUDIT OBJECTIVE

To assess the effectiveness of DTMB's efforts to establish an effective governance structure over the State's Oracle database environment.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Establishment of the Database Standards Committee to develop policies and procedures for the State's Oracle databases.

- Issuance of Oracle database policies and procedures that provided guidance on some database management and minimum configuration requirements.

- Material condition related to the need for a formal training program and reportable conditions related to the establishment of security policies and procedures and the management of software licenses for Oracle databases.

FINDING #3

A formal training program would help ensure that DBAs effectively manage databases.

DTMB did not establish a formal training program or take other steps to ensure that all DBAs managing the State's Oracle databases received sufficient training. A training program would help ensure that DBAs have the knowledge and skills to effectively manage a secure Oracle database environment. The lack of training, especially related to the security of Oracle databases, could have contributed to the exceptions noted in Findings #1 and #2.

According to Control Objectives for Information and Related Technology* (COBIT), training programs should be developed and delivered based on organizational and process requirements, including requirements for enterprise knowledge, internal control*, ethical conduct, and security. Also, COBIT states that employees should be provided with ongoing learning and opportunities to maintain their knowledge, skills, and competencies at a level required to achieve enterprise goals.

Survey responses from 33 (80%) of the 41 DBAs regarding their Oracle database training and experience disclosed:

Survey results from DBAs identified the lack of formal training and suggested potential training topics.

a. Nine (27%) of the 33 DBAs indicated that they had not received any training on the versions of Oracle database that they were managing. Of the 24 that had received training, 17 (71%) indicated that they had not received any training within the last year.

b. Twenty-eight (85%) of the 33 DBAs indicated that the State does not require that they attend training related specifically to Oracle database security.

c. Twenty-eight (85%) of the 33 DBAs indicated that they have not received the training necessary to perform their job effectively in all areas or have not received any training from the State. Twenty-three (82%) of those 28 DBAs suggested areas in which additional training was needed. Of those 23, 12 (52%) believed that they needed additional training in the security of Oracle databases.

DBAs are responsible for implementing and enforcing security and access controls over the State's Oracle databases, including those databases that support applications critical to State government operations. DTMB informed us that training is provided to DBAs at management's discretion when funding is available.

RECOMMENDATION

We recommend that DTMB establish a formal training program or take other steps to ensure that all DBAs managing the State's Oracle databases receive sufficient training.

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

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB will conduct a training needs analysis to identify gaps in employee training and related training needs. Upon completion, DTMB will develop an enterprise training program for all DBAs.

FINDING #4

Fully established security policies and procedures would help protect the State's databases.

DTMB did not fully establish policies and procedures for the security of the State's Oracle databases. As a result, DTMB cannot ensure that Oracle databases were securely configured to protect the confidentiality and integrity of critical data stored within the databases. Also, DTMB cannot ensure that audit logs capture the critical information necessary to detect unauthorized activity within the databases. Findings #1 and #2 may have resulted from a lack of fully established policies and procedures.

COBIT recommends that management create a set of policies to direct the information technology control expectations regarding defining baseline configurations, internal control, security, and confidentiality.

DTMB had not fully established and documented:

a. Minimum baseline configuration requirements for Oracle database security and procedures.

`

DBAs should review Oracle database security configurations periodically or after making significant patches or upgrades to the databases. According to Center for Internet Security* (CIS) benchmarks, which are based on National Institute of Standards and Technology* (NIST) standards and Oracle recommendations, the operation of the Oracle database is governed by numerous parameters that are set in specific configuration files. Changes to these configuration files should be carefully considered and maintained.

b. Policies and procedures defining minimum Oracle audit log configurations.

The lack of sufficient audit logs may prevent management from effectively monitoring the databases to detect and correct harmful database activity. According to CIS benchmarks, the ability to review audit logs to determine the result of user actions is among the most important of all database security features.

c. A policy governing the use of production data in nonproduction environments and any controls that need to be in place to mitigate the associated risk.

The 5 nonproduction databases we reviewed all contained copies of production data. Three (60%) of these databases contained confidential production data.

According to ISO/IEC 27002:2005, the use of sensitive information for testing purposes should be avoided. If sensitive data is used for testing purposes, all sensitive details and

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

content should be removed or modified beyond recognition before use.

DTMB informed us that it established the Database Standards Committee in June 2013; however, the Committee had not yet addressed these security concerns.

RECOMMENDATION

We recommend that DTMB fully establish policies and procedures for the security of the State's Oracle databases.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB established the Database Standards Committee in June 2013, which produced the first issuance of DTMB Database Security Standard 1340.00.15 in June 2014. The Committee used NIST and COBIT information management standards and Oracle best practices during preparations of this initial standard and will add the use of the CIS benchmark. DTMB held State of Michigan All DBA Workshops in 2013 and 2014, focused on the new 1340.00.15 standard and procedures. DTMB will expand the membership and assignments of the Committee to more rapidly create additional identified standards and procedures. Additional standards will be included for: 1) data masking of sensitive data in nonproduction databases; 2) additional audit logging and monitoring; and 3) additional database configuration baseline controls. DTMB will use its established Database Security Program Office to perform periodic reviews of adherence to these security standards throughout each year in all supported agencies. This program will ensure that an enterprise integrated approach to protecting sensitive information from inappropriate exposure or loss will be maintained.

FINDING #5

An improved system is necessary to help ensure proper database software license allocation and inventory accuracy.

DTMB should consider implementing a real-time system to manage its inventory of Oracle database software licenses to help ensure proper allocation of Oracle software licenses and accurate information in inventory records.

According to COBIT, entities should regularly perform checks and reconciliations of their software licensing inventory, including using software discovery tools. Also, COBIT states that an up-to-date and accurate inventory of licenses will help ensure that licensing compliance requirements are met and that license management is aligned with financial goals. A real-time system to manage the Oracle database software license inventory would be more efficient than DTMB's current manual inventory process.

Our review of the Oracle database software license inventory disclosed that DTMB:

a. Did not account for or allocate licenses to 5 operational servers that had Oracle installed on them and required licensure.

b. Allocated licenses to 5 nonoperational servers that did not have Oracle installed and did not require licensure.

c. Did not allocate a license to account for all instances of software in use by license type.

   For example, DTMB allocated a license to one server but had not allocated a license for each type of software in use on that server and had not requested that Oracle convert excess licenses of other types in the State's inventory into the license types necessary to cover the shortages.

d. Did not maintain accurate information, such as server host name, for all servers allocated a license in the inventory.

DTMB holds excess Oracle database software licenses in inventory. Therefore, the total number of licenses in use did not exceed the total number of licenses purchased from Oracle. However, licenses were not always allocated correctly based on inventory records.

Oracle makes its software available for download by the State's DBA teams before licenses have been allocated for use. DTMB uses a spreadsheet to manually track the allocation of its Oracle license inventory. DTMB relies on communication between the DBA teams and the DTMB licensing compliance manager and also an annual inventory audit performed by the licensing compliance manager to allocate licenses and make updates to the inventory. Any changes to the State's Oracle database environment that the DBA teams do not voluntarily report to the licensing compliance manager during the year will not be included in the inventory spreadsheet until the next annual inventory audit is completed. Delays in updating the inventory limit DTMB's ability to make inventory management decisions.

RECOMMENDATION

We recommend that DTMB consider implementing a real-time system to manage its inventory of Oracle database software licenses.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB recognizes the need to implement a real-time system to manage its inventory of Oracle database software licenses. DTMB is currently conducting a review of existing tools and processes to improve overall software asset management as a whole. Recommendations for improvements and any required funding requests will be presented to DTMB senior management.

DESCRIPTION

A database is a collection of information organized so that it can be easily accessed, managed, and updated. A database management system (DBMS), such as Oracle Database, is a software system that uses a standard method of cataloging, retrieving, and running queries on data. A DBMS manages input data, organizes the data, and provides ways for the data to be modified or extracted by users or other programs.

The State maintains approximately 500 Oracle databases that are used for transaction processing and reporting by the State's various information technology systems. Some of these databases contain confidential information and are classified as critical to State operations.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

Our audit scope was to examine the program and other records related to the State's Oracle database controls. We conducted this performance audit* in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit did not include a review of controls over the operating systems used for Oracle databases. Weaknesses at the operating system level could result in security vulnerabilities impacting Oracle databases.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered the period October 1, 2012 through September 30, 2014.

METHODOLOGY

We conducted a preliminary survey of DTMB's controls over Oracle databases. This included obtaining an understanding of DTMB policies and procedures for Oracle database security. We also reviewed the governance structure over Oracle databases, including policies and procedures for managing the State's Oracle databases, training and background requirements for DBAs, Oracle database tracking and licensing procedures, and the DBA team structure. We used the results of our preliminary survey to determine the extent of our detailed analysis and testing.

OBJECTIVE #1

To assess the effectiveness of DTMB's efforts to implement security and access controls over the State's Oracle databases.

To accomplish our first objective, we:

- Interviewed DBAs to obtain an understanding of the security and access controls implemented for Oracle databases.

- Judgmentally selected 7 production and 5 nonproduction Oracle databases and tested the configuration of the databases against industry best practices and DTMB standards. We judgmentally selected the databases for testing based on their significance to State operations.

- Tested the appropriateness of user access to the selected Oracle databases.

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

OBJECTIVE #2

To assess the effectiveness of DTMB's efforts to establish an effective governance structure over the State's Oracle database environment.

To accomplish our second objective, we:

- Reviewed and assessed DTMB's standards and guidance for securing Oracle databases.
- Obtained a listing of the State's Oracle databases and confirmed the accuracy and completeness of the listing with the DBAs and DTMB management.
- Solicited feedback from the DBAs and DTMB management regarding administration of the State's Oracle databases, including DBA training, policies and procedures, and the organizational structure of DBAs and DTMB managers responsible for the databases.
- Reviewed the Oracle contract to determine the method used to calculate annual support fees that the State pays Oracle for software updates and technical support.
- Reviewed Oracle license allocation and evaluated the number of excess licenses and the associated cost.

CONCLUSIONS

We based our conclusions on our audit efforts as described in the preceding paragraphs and the resulting material conditions and reportable conditions noted in the background, findings, and recommendations section. The material conditions are more severe than a reportable condition and could impair management's ability to operate effectively or could adversely affect the judgment of an interested person concerning the effectiveness of the State's Oracle databases. The reportable conditions are less severe than a material condition but represent deficiencies in internal control.

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

AGENCY RESPONSES

Our audit report contains 5 findings and 5 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 DTMB to develop a plan to comply with the audit 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.

GLOSSARY OF ABBREVIATIONS AND TERMS

access controls

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

availability

Timely and reliable access to data and information systems.

baseline configuration

A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Center for Internet Security (CIS)

A not-for-profit organization that establishes and promotes the use of consensus-based best practice standards to raise the level of security and privacy in information technology systems.

confidentiality

Protection of data from unauthorized disclosure.

configuration

The way a system is set up. Configuration can refer to either hardware or software or the combination of both.

configuration management

The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.

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.

database

A collection of information that is organized so that it can be easily accessed, managed, and updated.

database administrator (DBA)

The person responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users of the database. Additional responsibilities include operation, performance, integrity, and security of the database.

database management system (DBMS)

Software that uses a standard method of cataloging, retrieving, and running queries on data. The DBMS manages incoming data, organizes the data, and provides ways for the data to be modified or extracted by users or other programs.

data custodian

An individual or organization that has responsibility delegated by a data owner for maintenance or technological management of data and systems.

data owner

An individual or organization, usually a member of senior management of an organization, who is ultimately responsible for ensuring the protection and use of data.

DTMB

Department of Technology, Management, and Budget.

effectiveness

Success in achieving mission and goals.

Federal Information System Controls Audit Manual (FISCAM)

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

integrity

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

internal control

The organization, policies, and procedures adopted by management and other personnel to provide reasonable assurance that operations, including the use of 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 assets against unauthorized acquisition, use, or disposition.

ISO/IEC 27002:2005

A security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in the standard provide general guidance on the commonly accepted goals of information security management.

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.

National Institute of Standards and Technology (NIST)

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

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.

principle of least privilege

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

reportable condition

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

security

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

segregation of duties

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

vulnerability

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

This Page Left Intentionally Blank

OAG

Office of the Auditor General

Independent Objective Transparent