Office of the Auditor General
Performance Audit Report

Statewide Microsoft SQL Database Controls

Department of Technology, Management, and Budget

June 2020

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

071-0571-19

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

The auditor general may make investigations pertinent to the conduct of audits.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit

Statewide Microsoft SQL Database Controls

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0571-19

Released:
June 2020

DTMB maintains approximately 4,200 Microsoft SQL databases that State agencies use for transaction processing and reporting by the State's various IT systems. DTMB Agency Services includes database administrator (DBA) teams that manage the SQL databases. 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 governance structure over the Microsoft SQL database environment.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB needs improvements to its governance over the State's Microsoft SQL database environment to help address the root cause of the findings reported under Objective #2 (Finding #1).	X		Agrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of DTMB's efforts to implement key security and access controls over the State's Microsoft SQL databases.	Not effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
Ninety-two percent of databases tested were operating without the most current recommended Microsoft patch applied. The number of days since the last patch applied ranged from 20 days to 5.2 years (Finding #2).	X		Agrees
All databases tested had configuration settings not compliant with Center for Internet Security benchmark recommendations (Finding #3).	X		Agrees

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
Forty-six percent of databases tested did not have encryption-in-transit turned on to minimize the risk of sensitive or confidential data being inadvertently disclosed or accessed during transmission (Finding #4).	X		Agrees
None of the DBA teams selected were aware of new vulnerability management processes that DTMB had implemented. Also, over half of the DBAs and their supervisors did not have access to the new scanning tool. In addition, 50% of tested databases had vulnerabilities that were not remediated in a timely manner (Finding #5).	X		Agrees
Ninety-two percent of the DBA teams sampled could not provide evidence of periodic user database account recertification to ensure that access was still necessary or appropriate. Thirty-three percent of the user accounts reviewed either no longer required access or had excessive privileges. Also, 60% of tested DBAs were using a privileged account that did not have appropriate password complexities (Finding #6).	X		Agrees
Eighty-three percent of the DBA teams selected did not fully monitor high-risk privileged and non-privileged user activity on the database. Also, 50% of the DBA teams selected did not enable audit logging. In addition, 83% of the DBA teams selected did not define high-risk events that, when triggered, would generate an alert (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

June 9, 2020

Mr. Brom Stibitz
Acting Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Mr. Stibitz:

This is our performance audit report on Statewide Microsoft SQL Database 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 to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

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

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

STATEWIDE MICROSOFT SQL DATABASE CONTROLS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

GOVERNANCE STRUCTURE

BACKGROUND

Agency Services, Department of Technology, Management, and Budget (DTMB), manages the State's Microsoft SQL database* environment. Teams of database administrators* (DBAs) are responsible for the day-to-day operation, configuration*, and security* of their assigned databases.

AUDIT OBJECTIVE

To assess the effectiveness* of DTMB's governance structure over the Microsoft SQL database environment.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- DTMB implemented some standards and procedures related to Microsoft SQL database administration.
- DTMB conducted vulnerability* scans of most of the Microsoft SQL databases.
- Some DBA teams have developed and implemented some internal procedures.
- One material condition* related to improved governance over the State's Microsoft SQL database environment (Finding #1).

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

FINDING #1

Improvements in governance needed.

DTMB should improve its governance over the State's Microsoft SQL database environment. Fully mature governance ensures efficient and effective IT operations through clear and well-defined IT business processes, appropriate internal control*, and accountability for decision-making. In addition, improvements to IT governance would help DTMB address the root cause of the findings reported under Objective #2.

According to the IT Governance Institute* (ITGI) and Control Objectives for Information and Related Technology* (COBIT), effective governance includes:

- Assignment of roles, responsibilities, authority, and accountability.
- Development, maintenance, and communication of policies, standards, and procedures.
- Processes to monitor and test compliance with policies, procedures, and security performance metrics and report results to upper management.
- Education and training of security requirements, processes, and management expectations.

DTMB could improve its governance process by:

a. Developing more detailed operational guidance for implementing the State of Michigan (SOM) technical standards and procedures.

   SOM Technical Standard 1305.00.01 requires that procedures be a series of step-by-step instructions defining "who does what" and "how" it is to be done. According to ITGI, procedures must be clear and unambiguous and contain all necessary steps needed to accomplish the task.

   Based on our review of SOM technical procedures and information from the DBA teams, SOM technical procedures are written at an enterprise level and do not always fully communicate the step-by-step processes or fully provide the guidance needed by DBAs and their supervisors to perform their job responsibilities.

   Additional guidance will help to remediate the deficiencies identified in Finding #2, Finding #3, and Finding #7.

b. Providing training on internal processes and procedures.

   According to COBIT, training programs should be developed and delivered based on organizational and process requirements, including requirements for

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

enterprise knowledge, internal control, ethical conduct, and security. Also, COBIT states that employees should be provided with ongoing learning opportunities to maintain their knowledge, skills, and competencies at a level required to achieve enterprise goals.

Training in internal processes and procedures would help those individuals responsible for database administration better understand and adhere to SOM technical standards and procedures and help remediate the deficiencies identified in Finding #5.

c. Defining and communicating roles, responsibilities, and management expectations of DBAs and DBA supervisors.

COBIT states that organizations should establish and communicate roles and responsibilities to ensure accountability. Also, organizations should implement adequate supervisory practices to ensure that roles and responsibilities are properly exercised and assess whether individuals have sufficient resources to execute their roles and responsibilities.

Our interviews with DBAs and their supervisors disclosed inconsistences in their understanding of their roles and responsibilities and management's expectations.

d. Developing processes to monitor and assess compliance with SOM technical standards and procedures and adopted industry best practices, including processes for:

Additional monitoring and compliance assessments essential for success.

(1) Configuration security management*.

(2) Encryption-in-transit.

(3) Access controls*.

According to COBIT, organizations should implement processes to monitor and assess compliance with standards and procedures. Also, COBIT states that management should audit the process, evaluate performance by assessing against an organization's standards and procedures, identify gaps, and implement corrective action.

Developing these processes will help DTMB remediate the deficiencies identified in Finding #3, Finding #4, Finding #6, and Finding #7.

e. Fully communicating available data that management could use for improved monitoring and reporting.

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

COBIT states that organizations should ensure that pertinent information is identified, captured, and communicated in a form and time frame that enables people to carry out their responsibilities. Also, organizations should ensure that communication and reporting mechanisms provide appropriate information to those responsible for oversight and decision-making.

DTMB's Agency Services was not fully aware of all database attributes that were available for reporting, such as database type, name, and number of databases and database instances* residing on a server.

Within a database server environment, a network server may have one or more database instances residing on a network server and each instance may consist of one or more databases. Each database instance and database will have its own set of security configuration settings and user access controls. Therefore, it is important for DTMB to capture and use this level of detail to ensure that management can appropriately monitor and provide oversight in areas such as security configuration, patch* management, vulnerability management, and encryption.

We consider this finding to be a material condition because of the importance of IT governance. Insufficient IT governance resulted in the high number of weaknesses reported in the findings under Objective #2. With more effective oversight, DTMB can help mitigate risks to the State's database environment and the data stored within it.

RECOMMENDATION

We recommend that DTMB improve its governance over the State's Microsoft SQL database environment.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the need for strong governance and will improve the communication of responsibilities for promoting compliance with the State's technical standards and procedures to DBAs and DBA managers. In addition, DTMB will develop reports to monitor ongoing compliance with State technical standards and procedures and will communicate the availability of these reports.

DTMB is rightsizing the State's security standards and procedures and developing a set of tailored National Institute of Standards and Technology (NIST) control baselines to ensure that the controls for each information system are appropriate for the information types that it processes. This process will implement the NIST Risk Management Framework.*

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

Even after rightsizing the State's security standards and procedures, the complexity of the State's business and technical environment will require time and may require additional resources, funding, and tools for DTMB to implement the organizational actions that DTMB identified in its responses to the other findings contained in this audit report. DTMB will identify the activities that it can perform within its existing resources, then assess the additional resources and potential funding required to implement the processes that DTMB identified in its responses to the other findings contained in the audit report.

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. Weak database management system* (DBMS) security not only compromises the database but also may compromise the operating system and other trusted network systems. The State's Microsoft SQL database security and access controls are the responsibility of the DBA teams in conjunction with data owners at the various State agencies.

In a Microsoft SQL database environment, databases may have their own unique security configurations and user access controls but, generally, they inherit their security configuration and access controls from the instance they reside on.

AUDIT OBJECTIVE

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

CONCLUSION

Not effective.

FACTORS IMPACTING CONCLUSION

- Six material conditions related to applying patches in a timely manner, implementing effective security configuration controls, ensuring that encryption-in-transit is enabled, improving procedures for scanning vulnerabilities, establishing effective user access controls, and implementing effective monitoring processes (Findings #2 through #7).

- Implementation of some security configurations in accordance with State policy and adopted industry best practices.

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

FINDING #2

DTMB did not apply all required Microsoft SQL database patches in a timely manner to ensure that the State's data is protected from known security threats* and vulnerabilities.

Improved timeliness of patching needed.

Patches correct security and functionality vulnerabilities in the database software. SOM Technical Standard 1340.00.150.01 specifies the time frames in which security patches must be applied. According to NIST, applying patches is essential to reducing the opportunity for exploitation.

92% of databases did not have a current patch installed, ranging from 20 days to 5.2 years since the last patch installation.

We reviewed DTMB's patch management process for a judgmental sample of 24 databases. We noted that 22 (92%) of the databases did not have the most current patch installed and did not have a documented and approved business case for not applying the patch. The number of days since the databases were last patched ranged from 20 days to 5.2 years as of September 20, 2019. Because of the confidential and sensitive nature of database patching, we summarized our testing results for presentation in the finding and provided the detailed results to DTMB management.

Various types of patches are released by the vendors for databases. SOM Technical Standard 1340.00.150.01 does not provide sufficient detailed guidance to enable DBAs to determine the types of patches that need to be applied upon release. This lack of guidance and lack of formal procedures contributed to the deficiencies noted.

We consider this finding to be a material condition because of the number of weaknesses identified and the importance of patch management in mitigating risk to data stored within the databases. Patch management is an industry best practice for protecting against vulnerabilities.

RECOMMENDATION

We recommend that DTMB apply all required Microsoft SQL database patches in a timely manner to ensure that the State's data is protected from known security threats and vulnerabilities.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees that it should apply security patches to Microsoft SQL databases in accordance with State technical standards. DTMB will assess the need to update the State's technical standard and to develop clear guidance on patch management for Microsoft SQL databases. State technical standards do not currently provide clear guidance on the process associated with functional patches. DTMB will differentiate between security and functional patches and provide clear guidance on processes for critical patches and other patches and apply an appropriate standard to both.

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

DTMB reduces the risk to the State's data from known security threats and vulnerabilities by ensuring that databases reside in restricted trusted internal security zones, protected by firewalls and firewall rules specific to each application and database, in conjunction with intrusion protection, antivirus software, and State of Michigan standard security safeguards. In addition, operating system logs are monitored for suspected security violations, suspicious activities, and unusual actions and correlated across the organization. DTMB also requires security software on workstations to identify potential threats or abnormal user activity on State computers.

The complexity of the State's business environment requires DTMB to partner with State agencies to implement security patches. State agency business needs require blackout periods where changes to databases are not generally permitted for certain applications, preventing DTMB from always implementing security patches in accordance with State technical standards. In addition, State agency personnel are often required to participate in testing. State agencies fund DTMB DBA positions and, therefore, State agency business priorities often determine the work activities of DBAs. DBAs often need to balance State agency priorities with DTMB priorities.

To increase DTMB's ability to apply Microsoft SQL database security patches in accordance with State technical standards:

- *DTMB completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational security patch management improvements via a Lean Process Improvement, similar to Six Sigma (January and February 2020). DTMB will assess resource and potential funding requirements necessary to implement the new organizational processes before formalizing the new processes within standard operating procedures.*

- *DTMB granted access to the vulnerability management tool to DBAs and their managers for the purpose of tracking security patch status for the database servers they support (January 2020).*

DTMB implemented ongoing training for personnel in the use of the vulnerability scanning tool and the vulnerability management process, including identifying missing security patches. All active DBAs have attended this training.

FINDING #3

Improvements in Microsoft SQL database security configuration needed.

DTMB did not fully implement effective Microsoft SQL database security configuration controls in accordance with SOM technical standards, technical procedures, and adopted industry best practices. Properly configured databases reduce the risk of unauthorized access to the State's data, thereby protecting it from unauthorized modification, loss, or disclosure.

NIST states that organizations should establish and implement the most restrictive settings appropriate for the operational environment. Also, SOM Technical Standard 1340.00.060.02 and SOM Technical Procedure 1340.00.060.02.02 specify that DTMB must follow security parameters from the Center for Internet Security* (CIS) benchmarks and that DBAs are required to set appropriate database security configurations.

We assessed 764 security configurations' settings for 24 judgmentally sampled databases. Our review disclosed:

100% of sampled databases were not fully compliant with CIS benchmarks.

- All 24 databases had at least one configuration setting that was not compliant with CIS benchmark recommendations.
- Of the 764 settings tested within the 24 selected databases, 207 (27%) were not set in accordance with CIS benchmarks.

Subsequent to bringing this finding to management's attention, DTMB indicated that it began the process of enabling appropriate security configuration settings or obtaining Technical Review Board (TRB) exceptions, as necessary.

Although SOM technical standards and procedures indicate that CIS benchmarks must be followed, they allow for great flexibility by stating that each database will be evaluated for appropriate security configurations and implemented as required. Because there are between 39 and 42 CIS benchmark configuration recommendations, depending on the database version, this level of flexibility causes uncertainty among DBA teams regarding which CIS benchmark settings are appropriate and should be implemented within their unique environments. DTMB could improve compliance with SOM technical standards and procedures by developing and communicating the minimum enterprise security baseline configurations. Also, DTMB had not developed detailed processes to monitor compliance with SOM technical standards and procedures. DTMB informed us that it will implement a scanning process to help ensure compliance with selected security configurations.

We consider this finding to be a material condition because of the number of weaknesses identified and the importance of these controls in ensuring the secure configuration of databases.

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

RECOMMENDATION

We recommend that DTMB fully implement effective Microsoft SQL database security configuration controls in accordance with SOM technical standards, technical procedures, and adopted industry best practices.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees to implement effective Microsoft SQL database configuration controls appropriate for the operational and business needs of the organization.

DTMB is rightsizing the State's security standards and procedures and developing a set of tailored NIST control baselines to ensure that the controls for each information system are appropriate for the information types it processes. This process will implement the NIST Risk Management Framework.

DTMB reduces the risk by ensuring that databases reside in restricted trusted internal security zones, protected by firewalls and firewall rules specific to each application and database, in conjunction with intrusion protection, antivirus software, and State of Michigan standard security safeguards.

Although individual information systems have applied secure configurations for Microsoft SQL databases, DTMB agrees to establish, document, and monitor the implementation of an organization-wide security configuration for all Microsoft SQL databases using the appropriate benchmark, which may be tailored to meet the operational and business needs of the organization.

DTMB has already completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational security configuration management improvements via a Lean Process Improvement, similar to Six Sigma (January and February 2020).

Even after rightsizing the State's security standards and procedures, the complexity of the State's business and technical environment will require time and may require additional resources, funding, and tools for DTMB to standardize and monitor the implementation of a secure configuration for Microsoft SQL databases across the organization. DTMB will identify the activities that it can perform within its existing resources, then assess the additional resources and potential funding required to implement a secure configuration of Microsoft SQL databases across the organization.

FINDING #4

Improvements needed over encryption-in-transit.

DTMB should ensure that encryption-in-transit is enabled for data transmitted to and from Microsoft SQL databases to minimize the likelihood that sensitive or confidential information will be inadvertently disclosed or accessed during transmission.

Encryption is the conversion of data into an unreadable format. SOM Technical Standard 1340.00.170.03 requires that encryption be enabled for SQL connections when data is transmitted.

Encryption-in-transit not enabled for 46% of selected databases.

We judgmentally sampled 24 State agency databases. For 11 (46%) of the 24 databases, encryption-in-transit was not properly configured. When enabled, this setting ensures that encryption-in-transit is applied to the transmission of data to and from the database. DTMB did not obtain a TRB exception for any of the 11 instances in which encryption-in-transit was not being enabled.

Subsequent to bringing this finding to management's attention, DTMB indicated that it began the process of enabling encryption-in-transit or obtaining TRB exceptions.

We consider this finding to be a material condition because of the number of weaknesses identified and the importance of data encryption in preventing unauthorized users from reading sensitive and confidential data as it travels to and from the database.

RECOMMENDATION

We recommend that DTMB ensure that encryption-in-transit is enabled for data transmitted to and from Microsoft SQL databases.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees to enable and monitor Microsoft SQL database encryption-in-transit appropriate for the operational and business needs of the organization.

DTMB reduces the risk by ensuring that databases reside in a restricted trusted internal security zone through DTMB's standard server deployment process. In the majority of cases, the unencrypted portion of communications with database servers does not take place over an undetectably interceptable connection, due to their location in a virtual hosting environment within secured facilities, behind a series of firewalls.

Establishing encryption in transit on database servers could (in limited cases) impact the ability of State agencies to provide required services to citizens and governmental and business users and, therefore, DTMB will perform an impact assessment and coordinate with State agencies to reduce the potential risk. Based on the impact assessment, DTMB will determine a timeline for establishing that encryption-in-transit for data transmissions to and from Microsoft SQL databases is enabled.

Monitoring that encryption in transit, where technically and operationally feasible, is enabled across the organization will require time and may require additional resources and funding. DTMB will identify the activities it can perform within its existing resources, then assess the additional resources and potential funding required to promote compliance with enabling encryption-in-transit for data transmissions to and from Microsoft SQL databases across the organization.

FINDING #5

Vulnerability management procedures need improvement.

DTMB did not fully establish and implement effective procedures to ensure that all Microsoft SQL databases were scanned for vulnerabilities and that the vulnerabilities were remediated in a timely manner.

DTMB Technical Standard 1340.00.150.01 requires that vulnerability scanning tools be employed and vulnerabilities be remediated within the required time frames based on their severity.

In 2018, DTMB implemented a new scanning tool to identify database vulnerabilities. Prior to 2018, DTMB's Technical Services and DTMB Michigan Cyber Security (MCS) performed vulnerability scans of the databases and notified the appropriate Agency Services group, which coordinated the remediation with the DBAs. DTMB informed us that, with the implementation of the new scanning tool, DBAs should view the scan results within the tool and begin remediating the vulnerabilities.

We judgmentally selected 24 databases managed by 12 DBA teams. Our review disclosed that DTMB did not:

a. Fully communicate the new vulnerability scanning and remediation process to the various DBA teams within DTMB's Agency Services.

None of the 12 DBA teams were aware of the new vulnerability management process.

None of the 12 DBA teams were aware of the new process. At the time of our audit, DBAs still expected DTMB's Technical Services or MCS to notify them of the vulnerability scan results if vulnerabilities were identified that the DBAs needed to remediate and assumed that there were no vulnerabilities if they were not notified.

b. Ensure that the DBAs and their supervisors had appropriate access to the new vulnerability scanning tool to view scan results:

(1) Fourteen (64%) of the 22 DBA supervisors did not have an account to access the scanning tool. Also, of the 8 DBA supervisors that had accounts, 5 (63%) had not accessed their account in over 30 days.

(2) Thirty-four (61%) of the 56 DBAs did not have an account to access the scanning tool. Of the 22 DBAs with accounts, 19 (86%) had not accessed their account in over 30 days.

Because the SOM Technical Standard requires vulnerability scans for all SOM networked servers at a minimum of every 30 days, DBAs should access their scanning tool account at least once every 30 days.

c. Ensure that vulnerabilities were remediated based on SOM Technical Standard 1340.00.150.01 requirements.

We noted:

(1) Two (8%) of the 24 databases selected did not have a vulnerability scan in the past 17 months. DTMB informed us that it scanned these databases using the old scanning tool prior to this period. However, the SOM Technical Standard requires a scan to be run at least monthly.

50% of selected databases had vulnerabilities that were not remediated timely, including 7 that were outstanding for more than 500 days.

(2) Eleven (50%) of the 22 databases selected had vulnerabilities that were not remediated within the required time frame of 15 to 90 days, depending on the severity, established by the SOM Technical Standard. We noted:

(a) All 42 vulnerabilities that were outstanding as of October 2, 2019 exceeded the required time frame for remediation. Seven vulnerabilities were outstanding for more than 500 days.

(b) For vulnerabilities that had been remediated, 11 (55%) of the 20 were not remediated in the required time frame of 60 to 90 days. On average, those database vulnerabilities were not remediated for 400 days.

DTMB did not fully communicate and train the DBAs in the new process and did not ensure that they had appropriate access to the new scanning tool.

We consider this finding to be a material condition because of the number of weaknesses identified and the importance of vulnerability management in ensuring the confidentiality, integrity, and availability of the information that resides in the State's database environment.

RECOMMENDATION

We recommend that DTMB fully establish and implement effective procedures to ensure that all Microsoft SQL databases are scanned for vulnerabilities and that the vulnerabilities are remediated in a timely manner.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the need to scan and remediate Microsoft SQL vulnerabilities based on risk and where appropriate for operational and business needs of the organization.

DTMB reduces the risk to the State's data from known security threats and vulnerabilities by ensuring that databases reside in restricted trusted internal security zones, protected by firewalls and firewall rules specific to each application and database, in conjunction with intrusion protection, antivirus software, and State of Michigan standard security safeguards. In addition, operating system logs are monitored for suspected security violations, suspicious activities, and unusual actions and correlated across the organization. DTMB also requires security software on workstations to identify potential threats or abnormal user activity on State computers.

The complexity of the State's business environment requires DTMB to partner with State agencies to remediate vulnerabilities. State agency business needs require blackout periods where changes to databases are not generally permitted for certain applications, preventing DTMB from always remediating vulnerabilities in accordance with State Technical Standards. In addition, State agency personnel are required to participate in testing. State agencies fund DTMB DBA positions and, therefore, State agency business priorities often determine the work activities of DBAs. DBAs often need to balance State agency priorities with DTMB priorities.

DTMB is assessing a risk-based approach to identifying and remediating vulnerabilities so that DTMB can focus on the most critical vulnerabilities and reduce the State's risk profile.

To increase DTMB's ability to remediate Microsoft SQL vulnerabilities at an organizational level:

- *DTMB completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational vulnerability management improvements via a Lean Process Improvement, similar to Six Sigma (January and February 2020). DTMB will assess resource and potential funding requirements necessary to implement the new organizational processes before formalizing the new processes within standard operating procedures.*

- *DTMB granted access to the vulnerability management tool to DBAs and their managers for the purpose of tracking vulnerability status for the database servers they support (January 2020).*

- *DTMB implemented ongoing training for personnel in the use of the vulnerability scanning tool and the vulnerability management process, including identifying missing security patches. All active database administrators have attended this training.*

- *DTMB implemented automated scanning of the majority of the servers in the organization. DTMB's vulnerability management tool enables DBAs and DBA management to*

automate reporting for monitoring of Microsoft SQL vulnerabilities.

- *DTMB is developing a series of enterprise dashboards as part of its Enterprise Vulnerabilities Management implementation project to provide vulnerability metrics across the organization and at various organizational levels.*

FINDING #6

User access controls need improvement.

DTMB did not fully establish and implement effective user access controls over the State's Microsoft SQL databases to help prevent or detect inappropriate access to the State's data.

SOM Technical Standard 1340.00.020.01 requires the establishment of a process to control and document the assignment of access rights based on current job responsibilities and to allow access to be managed and periodically reviewed to ensure that access is based on the principle of least privilege*. Also, SOM Technical Standard 1340.00.080.01 defines password complexity requirements for non-privileged, privileged, and service accounts.

Privileged accounts* include system administrators, security roles, and account administrators. Service accounts are used by an application or service to interact with the operating system, database, or other applications.

We judgmentally selected 24 databases and reviewed the user access management process of the 12 responsible DBA teams. Our review disclosed that DTMB did not:

a. Periodically recertify database user accounts.

92% of DBA teams had no evidence of periodic account recertification.

Eleven (92%) of the 12 DBA teams could not provide evidence that they performed user access recertification. Account review and recertification help ensure that continued use of the account is needed.

b. Remove access to accounts in a timely manner or grant access based on the principle of least privilege:

33% of database user accounts no longer needed access or had excessive access privileges.

(1) Of 267 user accounts, 87 (33%) either no longer required access to the database because of changes to their job duties or had excessive database privileges.

(2) Of 167 service accounts, 56 (34%) no longer required access to the database or had excessive database privileges.

c. Fully establish controls over privileged user accounts.

DBAs may have two separate accounts, a non-privileged user account and a privileged account to perform database work. Privileged accounts require greater password complexity than a non-privileged account.

Six (60%) of 10 judgmentally selected DBAs used a privileged account that did not have appropriate password complexity as required by the SOM Technical Standard.

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

DTMB would need to fully develop processes to monitor the granting, removal, and periodic recertification of privileged and non-privileged users with database access to help ensure that it complied with the technical standards. Because DBAs viewed their activities as non-privileged, the accounts they used to perform database tasks were not configured with the appropriate password complexities.

We consider this finding to be a material condition because of the number of weaknesses identified and the importance of user access controls in ensuring that only appropriate individuals have access to data based on their job responsibilities.

RECOMMENDATION

We recommend that DTMB fully establish and implement effective user access controls over the State's Microsoft SQL databases.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees that it should recertify privileged database accounts and monitor that the accounts that DBAs use for their database work are in alignment with the State's technical standard. In addition, DTMB will issue privileged accounts to all DBAs.

DTMB is rightsizing the State's security standards and procedures and developing a set of tailored NIST control baselines to ensure that the controls for each information system are appropriate for the information types that it processes. This process will implement the NIST Risk Management Framework.

DTMB reduces the risk of inappropriate access to State data by ensuring that databases reside in restricted trusted internal security zones, protected by firewalls and firewall rules specific to each application and database, in conjunction with intrusion protection, antivirus software, and State of Michigan standard security safeguards. In addition, operating system logs are monitored for suspected security violations, suspicious activities, and unusual actions and correlated across the organization. DTMB also requires security software on workstations to identify potential threats or abnormal user activity on State computers.

DTMB is establishing a new organizational process to recertify DTMB user access to SQL databases and to monitor that the process is consistently implemented. The recertification process will identify whether DTMB users have access that is appropriate for their job responsibilities and remove access for DTMB users who no longer have a business need.

Even after rightsizing the State's security standards and procedures, the complexity of the State's business and technical environment will require time and may require additional resources, funding, and tools for DTMB to standardize the recertification process and to monitor that the process is consistently implemented across the organization. DTMB will

identify the activities that it can perform within its existing resources, then assess the additional resources and potential funding required to implement a recertification process for Microsoft SQL databases across the organization.

FINDING #7

Improvements needed over monitoring of privileged activity, high-risk events, and audit logs.

DTMB should fully implement effective monitoring processes over Microsoft SQL databases to ensure that high-risk events (such as suspected security violations, suspicious activities, and unusual actions) are captured and reviewed.

SOM Technical Standard 1340.00.040.01 requires high alerts to be defined and captured and the logs to be reviewed using a risk-based approach.

We reviewed the monitoring practices of 12 DBA teams responsible for managing 24 judgmentally sampled databases. DTMB did not:

83% of DBA teams did not monitor privileged and non-privileged high-risk user activity.

a. Ensure that DBA supervisors monitored the high-risk privileged activity of the DBAs and that DBAs monitored the high-risk activity of non-privileged users with direct access to the database for 10 (83%) of the 12 DBA teams.

   Monitoring of privileged activity may include the review of modified logs, changes to account privileges, and inappropriate access to confidential data. Monitoring of non-privileged user activity may include failed and successful log-on attempts.

83% of selected DBA teams had not defined alerts for high-risk events.

b. Define the high-risk events that, when triggered, would generate an alert for 10 (83%) of the 12 DBA teams.

   According to NIST, an organization should evaluate significant and relevant security audit events to meet its ongoing needs. SOM Technical Standard 1340.00.040.01 lists activities that could be monitored, such as user account management activities, use of administrator privileges, and security policy modifications.

50% of selected DBA teams did not enable audit logging.

c. Enable audit logging for 6 (50%) of the 12 DBA teams.

   Audit logs can assist DBAs in identifying suspicious behavior along with providing information useful for resolving these problems.

Some DBA teams did not enable logging or define high-risk events because of concerns over the storage space that the logs might use. Other DBA teams enabled default logging and believed it to be sufficient because the logs were readily available for review, if needed.

This finding represents a material condition because of the number of weaknesses identified and because of the lack of monitoring and accountability for all privileged DBA accounts. Privileged accounts are the most powerful and, if compromised or abused, could create a security risk.

RECOMMENDATION

We recommend that DTMB fully implement effective monitoring processes over Microsoft SQL databases.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees that it did not fully implement monitoring processes over SQL databases to ensure that high-risk events are captured and reviewed.

DTMB reduces the risk by ensuring that databases reside in restricted trusted internal security zones, protected by firewalls and firewall rules specific to each application and database, in conjunction with intrusion protection, antivirus software, and State of Michigan standard security safeguards. In addition, operating system logs are monitored for suspected security violations, suspicious activities, and unusual actions and correlated across the organization.

DTMB is rightsizing the State's security standards and procedures and developing a set of tailored NIST control baselines to ensure that the controls for each information system are appropriate for the information types it processes. This process will implement the NIST Risk Management Framework.

DTMB will perform an assessment to determine the resources and costs to expand the State's ability to capture and review high-risk events. The complexity of the State's business and technical environment may require additional resources, including funding, tools, and storage capacity, for DTMB to expand its ability to capture and review high-risk events. If funding is needed, DTMB will make a request in future budget cycles.

DESCRIPTION

A database is a stored collection of related data needed by enterprises and individuals to meet their information processing and retrieval requirements. A DBMS, such as Microsoft SQL, is a software system that controls the organization, storage, and retrieval of data in a database. The DBMS manages and organizes data and provides a method for the data to be modified or extracted by users or other programs. The DBMS permits centralized control of security and data integrity.

DTMB has 22 DBA supervisors and 56 DBAs who maintain the approximately 4,200 Microsoft SQL databases residing on approximately 290 database instances. The databases are used by State agencies for transaction processing and reporting by the State's various IT systems. Some of the databases contain confidential information and are classified as critical to the State's operations.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the program and other records related to the State's Microsoft SQL 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 Microsoft SQL databases. Weaknesses at the operating system level could result in security vulnerabilities impacting the databases.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2017 through February 29, 2020.

METHODOLOGY

We conducted a preliminary survey of DTMB's Microsoft SQL database controls. During our preliminary survey, we:

- Interviewed DTMB management and staff to gain an understanding of Microsoft SQL database controls.
- Reviewed DTMB policies and procedures related to Microsoft SQL database administration and security.
- Reviewed CIS Microsoft SQL database benchmarks.
- Obtained an understanding of DTMB's processes for:
    - Granting, monitoring, and removing user access to the Microsoft SQL databases.
    - Monitoring privileged user access.
    - Securing Microsoft SQL databases.
    - Training the DBAs.
    - Providing oversight for vulnerability management, patch management, and encryption.

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

OBJECTIVE #1

To assess the effectiveness of DTMB's governance structure over the Microsoft SQL database environment.

To accomplish this objective, we:

- Obtained a listing of the State's Microsoft SQL databases and confirmed the accuracy and completeness of the listing with DTMB management.
- Reviewed and assessed DTMB's standards and guidance for securing Microsoft SQL databases.
- Conducted a survey to solicit feedback from DBAs, DBA supervisors, and DTMB management regarding DBA training, policies and procedures, and the organizational structure.
- Reviewed Microsoft SQL database licensing contracts to verify extended support and consistency of rates being paid by departments.

OBJECTIVE #2

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

To accomplish this objective, we:

- Interviewed DBAs to obtain an understanding of the security and access controls implemented for Microsoft SQL databases.
- Judgmentally selected 12 of 21 DBA teams. We then judgmentally selected 1 production* and 1 nonproduction* database, as of August 2019, from each of the 12 teams and:
    - Tested the appropriateness of user access to selected databases.
    - Tested the database configurations against adopted industry best practices and DTMB standards.
    - Assessed the last login dates of vulnerability scanning tool accounts to determine whether DBAs were actively using the tool in accordance with their job responsibility.

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

- Reviewed database vulnerability reports to assess whether outstanding and mitigated vulnerabilities complied with DTMB standards for remediation.

- Identified current patch levels on Microsoft SQL databases and evaluated to vendor recommendations.

- Obtained database encryption-in-transit configurations and assessed whether the configurations enforce SOM policy.

- Validated that audit logs were enabled and captured information as required by SOM standards.

We made our selections using a risk-based approach. Because our selections were judgmental, we could not project our results to the population.

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 7 corresponding recommendations. DTMB's preliminary response indicates that it agrees with all 7 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 fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

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

GLOSSARY OF ABBREVIATIONS AND TERMS

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.
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 IT 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 security 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 IT.
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 instance	A specific installation of Microsoft SQL. It is not the database itself; rather, it is the software used to create 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.
DTMB	Department of Technology, Management, and Budget.

effectiveness	Success in achieving mission and goals.
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.
IT	information technology.
IT Governance Institute (ITGI)	A research think tank that is a leading resource on IT governance for the global business community. ITGI aims to benefit enterprises by assisting enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals. By conducting original research on IT governance and related topics, ITGI helps enterprise leaders understand and have the tools to ensure effective governance over IT within their enterprise.
material condition	A matter that, in the auditor's judgment, is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program. Our assessment of materiality is in relation to the respective audit objective.
MCS	Michigan Cyber Security.
Microsoft SQL database	A relational database management system that supports transaction processing, business intelligence, and analytics applications in IT environments. This is a Microsoft product.
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.
nonproduction database	A database used to develop, test, and evaluate changes before moving the changes to the production database.

patch	An update to an operating system, applications, or other software to correct particular problems with the software.
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.
privileged account	An account that has access to all commands and files on an operating system or database management system.
production database	A database used to process live data that is received as input in the production environment.
reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
SOM	State of Michigan.
SQL	Structured Query Language.
threat	An activity, intentional or unintentional, with the potential for causing harm to automated information system or activity.
TRB	Technical Review Board.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

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