STATE OF MICHIGAN

GRETCHEN WHITMER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

BROM STIBITZ
DIRECTOR

October 14, 2021

Mr. Richard Lowe, Chief Internal Auditor
Office of Internal Audit Services
Office of State Budget
George W. Romney Building
111 South Capitol, 6th Floor
Lansing, Michigan 48933

Dear Mr. Lowe:

In accordance with the State of Michigan, Financial Management Guide, Part VII, as initially submitted on 8/7/2020, following is a summary table identifying our ongoing responses and corrective action plans to address recommendations contained within the Office of the Auditor General's audit report of Statewide Microsoft SQL Database Controls (071-0571-19).

If you have any questions, or if we can be of further assistance, please don't hesitate to contact me directly.

Sincerely,

Brom Stibitz
DTMB Director
& Chief Information Officer
DTMB

Attachment: DTMB Corrective Action Plan Response to OAG Statewide Microsoft SQL Database Controls audit (071-0571-19)

CC: Senator Edward McBroom, Senate Oversight Committee
Representative Steve Johnson, House Oversight Committee
Senator Roger Victory, Chair, Senate Appropriations Subcommittee on General Government
Representative Greg VanWoerkom, Chair, House Appropriations Subcommittee on General Government
Zack Kolodin, Executive Office of the Governor
Doug Ringler, Auditor General
Michelle Lange, Chief Deputy Director
Laura Clark, Chief Security Officer
Jack Harris, Chief Technology Officer
Cindy Peruchietti, Director Agency Services
Eric Swanson, Director Center for Shared Solutions
Sherri Irwin, Director, Office of Support Services

DTMB Corrective Action Plan Response to OAG Statewide Microsoft SQL Database Controls audit (071-0571-19)

DTMB

Statewide Microsoft SQL Database Controls audit

Summary of Agency Responses to Recommendations

1. Audit recommendations DTMB fully remediated: None
2. Audit recommendations DTMB agreed with and remediation is in progress: #1, #2, #3, #4, #5, #6, #7
3. Audit recommendations DTMB disagreed with: None

DTMB's Responses to Recommendations:

Finding #1 – Governance

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 Technical Standards and Procedures and developing a set of tailored security control baselines based on the National Institute of Standards and Technology (NIST) control framework to ensure the controls for each information system are appropriate for the information types it processes (anticipated completion 2021). As part of this process, DTMB has developed a parameterized NIST control framework set (March 2020). DTMB is also reviewing and streamlining the State's Technical Standards and Procedures, and will identify appropriate evidence to confirm DTMB is complying with the new parameterized control framework and the State's Technical Standards and Procedures (anticipated completion 2021). This process will implement the NIST Risk Management Framework.

As part of the State's biennial Internal Control and Evaluation (ICE) process, DTMB is completing System Security Plans (SSP) for the State's general IT support systems and will identify the risks which will be remediated. DTMB will then identify the activities to remediate these risks and assess which activities DTMB can perform within our existing resources and which activities will require additional resources and potential funding.

The alignment of this effort with the upcoming ICE process will reduce rework and enable DTMB's strategic goal of the responsible use of Taxpayer revenue. DTMB will identify applicable controls for the State's general IT support systems and the standard appropriate evidence to confirm DTMB is complying with the new NIST control baseline and the State's Technical Standards and Procedures. The owner of each general IT support system will

generate appropriate audit evidence which will be reused for subsequent audits during the period until the next evaluation.

DTMB has also assigned an individual to update DTMB-IT executives regarding information technology audits and progress to reducing risks identified in OAG information technology audit reports.

Prior to the completion of the OAG's audit, DTMB completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational database management improvements via a Lean Process Improvement, similar to Six Sigma (January and February 2020). The Lean Process Improvement (LPI) teams are identifying the resource requirements and activities necessary to implement the improved processes identified in the LPI and to implement further risk reductions. These efforts will improve DTMB's security posture for databases.

DTMB has completed the following activities to improve governance and reduce risks identified in the audit:

Governance Activities:

- DTMB created an email distribution list to improve communication to DBAs across the organization (January 2020).
- DTMB has drafted an organizational approach to develop and maintain common and consistent database practices to improve compliance and security across the organization (July 2020).
- DTMB DBAs completed a survey identifying tools used for database management activities (93% participation) which can be used to promote governance through the standardization of tools and skills training (June 2020).
- DTMB reviewed and documented necessary updates to the State's Enterprise Database Standard 1340.00.060.02 Database Security Standard (June 2020).

Security and Access Control Activities:

Database security configurations:

- DTMB conducted working sessions identifying the process for the technical implementation of database security configuration scanning, with the initial focus on configuring the scanning tool and ensuring the tool can access the database servers (June 2020).

Encryption in transit:

- DTMB developed a script identifying whether encryption-in-transit is enabled for Microsoft SQL databases (November 2019).
- DTMB has drafted initial guidance to configure and enable Microsoft SQL database encryption-at-rest and encryption-in-transit (July 2020).

Vulnerability scanning:

- DTMB has 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 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 has 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 (May 2020).
- DTMB completed a high-level estimate to assess the resources necessary to remediate SQL server vulnerabilities (February 2020).

Privileged accounts:

- DTMB provisioned privileged accounts for DBAs who perform SQL server database administration activities (July 2020).
- DTMB developed guidance to DBAs for requesting a privileged account (July 2020).
- DTMB developed guidance for the use of privileged accounts for SQL server database administration (April 2020).

DTMB will also improve the communication of responsibilities for promoting compliance with the State's Technical Standards and Procedures to DBAs and DBA managers.

Even after rightsizing the State's Technical 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 DTMB identified in its responses to the other findings contained in this audit report. DTMB will identify the activities DTMB can perform within our existing resources, then assess the additional resources and potential funding required to implement further risk reductions.

Finding #2 – Patch Management

DTMB agrees 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.

DTMB reduces the risk to the State's data from known security threats and vulnerabilities by ensuring 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 rightsizing the State's Technical Standards and Procedures and developing a set of tailored security control baselines based on the National Institute of Standards and Technology (NIST) control framework to ensure the controls for each information system are appropriate for the information types it processes (anticipated completion 2021). As part of this process, DTMB has developed a parameterized NIST control framework set (March 2020). DTMB is also reviewing and streamlining the State's Technical Standards and Procedures, and will identify appropriate evidence to confirm DTMB is complying with the new parameterized control framework and the State's Technical Standards and Procedures (anticipated completion 2021). This process will implement the NIST Risk Management Framework.

As part of the State's biennial Internal Control and Evaluation (ICE) process, DTMB is completing System Security Plans (SSP) for the State's general IT support systems and will identify the risks which will be remediated. DTMB will then identify the activities to remediate these risks and assess which activities DTMB can perform within our existing resources and which activities will require additional resources and potential funding.

The alignment of this effort with the upcoming ICE process will reduce rework and enable DTMB's strategic goal of the responsible use of Taxpayer revenue. DTMB will identify applicable controls for the State's general IT support systems and the standard appropriate evidence to confirm DTMB is complying with the new NIST control baseline and the State's Technical Standards and Procedures. The owner of each general IT support system will generate appropriate audit evidence which will be reused for subsequent audits during the period until the next evaluation.

DTMB has also assigned an individual to update DTMB-IT executives regarding information technology audits and progress to reducing risks identified in OAG information technology audit reports.

Prior to the completion of the OAG's audit, DTMB completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational database management improvements via a Lean Process Improvement, similar to Six Sigma (January and February 2020). The Lean Process Improvement (LPI) teams are identifying the resource requirements and activities necessary to implement the improved processes identified in the LPI and to implement further risk reductions. These efforts will improve DTMB's security posture for databases.

DTMB has completed the following activities to improve governance and reduce risks identified in the audit:

Governance Activities:

- DTMB created an email distribution list to improve communication to DBAs across the organization (January 2020).

- DTMB has drafted an organizational approach to develop and maintain common and consistent database practices to improve compliance and security across the organization (July 2020).
- DTMB DBAs completed a survey identifying tools used for database management activities (93% participation) which can be used to promote governance through the standardization of tools and skills training (June 2020).
- DTMB reviewed and documented necessary updates to the State's Enterprise Database Standard 1340.00.060.02 Database Security Standard (June 2020).

Security and Access Control Activities:

Database security configurations:

- DTMB conducted working sessions identifying the process for the technical implementation of database security configuration scanning, with the initial focus on configuring the scanning tool and ensuring the tool can access the database servers (June 2020).

Encryption in transit:

- DTMB developed a script identifying whether encryption-in-transit is enabled for Microsoft SQL databases (November 2019).
- DTMB has drafted initial guidance to configure and enable Microsoft SQL database encryption-at-rest and encryption-in-transit (July 2020).

Vulnerability scanning:

- DTMB has 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 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 has 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 (May 2020).
- DTMB completed a high-level estimate to assess the resources necessary to remediate SQL server vulnerabilities (February 2020).

Privileged accounts:

- DTMB provisioned privileged accounts for DBAs who perform SQL server database administration activities (July 2020).
- DTMB developed guidance to DBAs for requesting a privileged account (July 2020).
- DTMB developed guidance for the use of privileged accounts for SQL server database administration (April 2020).

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 database administrator positions and therefore, State

Agency business priorities often determine the work activities of database administrators. DBAs often need to balance State Agency priorities with DTMB priorities. DTMB will identify the activities DTMB can perform within our existing resources, then assess the additional resources and potential funding required to apply security patches to Microsoft SQL databases in accordance with State Technical Standards across the organization.

Finding #3 – Security Configurations

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

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 reduces the risk by ensuring 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.

DTMB is rightsizing the State's Technical Standards and Procedures and developing a set of tailored security control baselines based on the National Institute of Standards and Technology (NIST) control framework to ensure the controls for each information system are appropriate for the information types it processes (anticipated completion 2021). As part of this process, DTMB has developed a parameterized NIST control framework set (March 2020). DTMB is also reviewing and streamlining the State's Technical Standards and Procedures, and will identify appropriate evidence to confirm DTMB is complying with the new parameterized control framework and the State's Technical Standards and Procedures (anticipated completion 2021). This process will implement the NIST Risk Management Framework.

As part of the State's biennial Internal Control and Evaluation (ICE) process, DTMB is completing System Security Plans (SSP) for the State's general IT support systems and will identify the risks which will be remediated. DTMB will then identify the activities to remediate these risks and assess which activities DTMB can perform within our existing resources and which activities will require additional resources and potential funding.

The alignment of this effort with the upcoming ICE process will reduce rework and enable DTMB's strategic goal of the responsible use of Taxpayer revenue. DTMB will identify applicable controls for the State's general IT support systems and the standard appropriate evidence to confirm DTMB is complying with the new NIST control baseline and the State's Technical Standards and Procedures. The owner of each general IT support system will

generate appropriate audit evidence which will be reused for subsequent audits during the period until the next evaluation.

DTMB has also assigned an individual to update DTMB-IT executives regarding information technology audits and progress to reducing risks identified in OAG information technology audit reports.

Prior to the completion of the OAG's audit, DTMB completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational database management improvements via a Lean Process Improvement, similar to Six Sigma (January and February 2020). The Lean Process Improvement (LPI) teams are identifying the resource requirements and activities necessary to implement the improved processes identified in the LPI and to implement further risk reductions. These efforts will improve DTMB's security posture for databases.

DTMB has completed the following activities to improve governance and reduce risks identified in the audit:

Governance Activities:

- DTMB created an email distribution list to improve communication to DBAs across the organization (January 2020).
- DTMB has drafted an organizational approach to develop and maintain common and consistent database practices to improve compliance and security across the organization (July 2020).
- DTMB DBAs completed a survey identifying tools used for database management activities (93% participation) which can be used to promote governance through the standardization of tools and skills training (June 2020).
- DTMB reviewed and documented necessary updates to the State's Enterprise Database Standard 1340.00.060.02 Database Security Standard (June 2020).

Security and Access Control Activities:

Database security configurations:

- DTMB conducted working sessions identifying the process for the technical implementation of database security configuration scanning, with the initial focus on configuring the scanning tool and ensuring the tool can access the database servers (June 2020).

Encryption in transit:

- DTMB developed a script identifying whether encryption-in-transit is enabled for Microsoft SQL databases (November 2019).
- DTMB has drafted initial guidance to configure and enable Microsoft SQL database encryption-at-rest and encryption-in-transit (July 2020).

Vulnerability scanning:

- DTMB has 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 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 has 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 (May 2020).
- DTMB completed a high-level estimate to assess the resources necessary to remediate SQL server vulnerabilities (February 2020).

Privileged accounts:

- DTMB provisioned privileged accounts for DBAs who perform SQL server database administration activities (July 2020).
- DTMB developed guidance to DBAs for requesting a privileged account (July 2020).
- DTMB developed guidance for the use of privileged accounts for SQL server database administration (April 2020).

Even after rightsizing the State's Technical 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 DTMB can perform within our 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 – Encryption-in-Transit

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

DTMB reduces the risk by ensuring 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.

DTMB is rightsizing the State's Technical Standards and Procedures and developing a set of tailored security control baselines based on the National Institute of Standards and Technology (NIST) control framework to ensure the controls for each information system are appropriate for the information types it processes (anticipated completion 2021). As part of this process, DTMB has developed a parameterized NIST control framework set (March 2020). DTMB is also reviewing and streamlining the State's Technical Standards and Procedures, and will identify appropriate evidence to confirm DTMB is complying with the new parameterized control framework and the State's Technical Standards and Procedures (anticipated completion 2021). This process will implement the NIST Risk Management Framework.

As part of the State's biennial Internal Control and Evaluation (ICE) process, DTMB is completing System Security Plans (SSP) for the State's general IT support systems and will identify the risks which will be remediated. DTMB will then identify the activities to remediate these risks and assess which activities DTMB can perform within our existing resources and which activities will require additional resources and potential funding.

The alignment of this effort with the upcoming ICE process will reduce rework and enable DTMB's strategic goal of the responsible use of Taxpayer revenue. DTMB will identify applicable controls for the State's general IT support systems and the standard appropriate evidence to confirm DTMB is complying with the new NIST control baseline and the State's Technical Standards and Procedures. The owner of each general IT support system will generate appropriate audit evidence which will be reused for subsequent audits during the period until the next evaluation.

DTMB has also assigned an individual to update DTMB-IT executives regarding information technology audits and progress to reducing risks identified in OAG information technology audit reports.

Prior to the completion of the OAG's audit, DTMB completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational database management improvements via a Lean Process Improvement, similar to Six Sigma (January and February 2020). The Lean Process Improvement (LPI) teams are identifying the resource requirements and activities necessary to implement the improved processes identified in the LPI and to implement further risk reductions. These efforts will improve DTMB's security posture for databases.

DTMB has completed the following activities to improve governance and reduce risks identified in the audit:

Governance Activities:

- DTMB created an email distribution list to improve communication to DBAs across the organization (January 2020).
- DTMB has drafted an organizational approach to develop and maintain common and consistent database practices to improve compliance and security across the organization (July 2020).
- DTMB DBAs completed a survey identifying tools used for database management activities (93% participation) which can be used to promote governance through the standardization of tools and skills training (June 2020).
- DTMB reviewed and documented necessary updates to the State's Enterprise Database Standard 1340.00.060.02 Database Security Standard (June 2020).

Security and Access Control Activities:

Database security configurations:

- DTMB conducted working sessions identifying the process for the technical implementation of database security configuration scanning, with the initial focus on configuring the scanning tool and ensuring the tool can access the database servers (June 2020).

Encryption in transit:

- DTMB developed a script identifying whether encryption-in-transit is enabled for Microsoft SQL databases (November 2019).
- DTMB has drafted initial guidance to configure and enable Microsoft SQL database encryption-at-rest and encryption-in-transit (July 2020).

Vulnerability scanning:

- DTMB has 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 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 has 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 (May 2020).
- DTMB completed a high-level estimate to assess the resources necessary to remediate SQL server vulnerabilities (February 2020).

Privileged accounts:

- DTMB provisioned privileged accounts for DBAs who perform SQL server database administration activities (July 2020).
- DTMB developed guidance to DBAs for requesting a privileged account (July 2020).
- DTMB developed guidance for the use of privileged accounts for SQL server database administration (April 2020).

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 DTMB can perform within our 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

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

DTMB is rightsizing the State's Technical Standards and Procedures and developing a set of tailored security control baselines based on the National Institute of Standards and Technology (NIST) control framework to ensure the controls for each information system are appropriate for the information types it processes (anticipated completion 2021). As part of this process, DTMB has developed a parameterized NIST control framework set (March 2020). DTMB is also reviewing and streamlining the State's Technical Standards and Procedures, and will identify appropriate evidence to confirm DTMB is complying with the new parameterized control framework and the State's Technical Standards and Procedures (anticipated completion 2021). This process will implement the NIST Risk Management Framework.

As part of the State's biennial Internal Control and Evaluation (ICE) process, DTMB is completing System Security Plans (SSP) for the State's general IT support systems and will identify the risks which will be remediated. DTMB will then identify the activities to remediate these risks and assess which activities DTMB can perform within our existing resources and which activities will require additional resources and potential funding.

The alignment of this effort with the upcoming ICE process will reduce rework and enable DTMB's strategic goal of the responsible use of Taxpayer revenue. DTMB will identify applicable controls for the State's general IT support systems and the standard appropriate evidence to confirm DTMB is complying with the new NIST control baseline and the State's Technical Standards and Procedures. The owner of each general IT support system will generate appropriate audit evidence which will be reused for subsequent audits during the period until the next evaluation.

DTMB has also assigned an individual to update DTMB-IT executives regarding information technology audits and progress to reducing risks identified in OAG information technology audit reports.

Prior to the completion of the OAG's audit, DTMB completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational database management improvements via a Lean Process Improvement, similar to Six Sigma (January and February 2020). The Lean Process Improvement (LPI) teams are identifying the resource requirements and activities necessary to implement the improved processes identified in the LPI and to implement further risk reductions. These efforts will improve DTMB's security posture for databases.

DTMB has completed the following activities to improve governance and reduce risks identified in the audit:

Governance Activities:

- DTMB created an email distribution list to improve communication to DBAs across the organization (January 2020).
- DTMB has drafted an organizational approach to develop and maintain common and consistent database practices to improve compliance and security across the organization (July 2020).
- DTMB DBAs completed a survey identifying tools used for database management activities (93% participation) which can be used to promote governance through the standardization of tools and skills training (June 2020).
- DTMB reviewed and documented necessary updates to the State's Enterprise Database Standard 1340.00.060.02 Database Security Standard (June 2020).

Security and Access Control Activities:

Database security configurations:

- DTMB conducted working sessions identifying the process for the technical implementation of database security configuration scanning, with the initial focus on configuring the scanning tool and ensuring the tool can access the database servers (June 2020).

Encryption in transit:

- DTMB developed a script identifying whether encryption-in-transit is enabled for Microsoft SQL databases (November 2019).
- DTMB has drafted initial guidance to configure and enable Microsoft SQL database encryption-at-rest and encryption-in-transit (July 2020).

Vulnerability scanning:

- DTMB has 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 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 has 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 (May 2020).

- DTMB completed a high-level estimate to assess the resources necessary to remediate SQL server vulnerabilities (February 2020).

Privileged accounts:

- DTMB provisioned privileged accounts for DBAs who perform SQL server database administration activities (July 2020).
- DTMB developed guidance to DBAs for requesting a privileged account (July 2020).
- DTMB developed guidance for the use of privileged accounts for SQL server database administration (April 2020).

DTMB is also 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.

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 database administrator positions and therefore, State Agency business priorities often determine the work activities of database administrators. DBAs often need to balance State Agency priorities with DTMB priorities. DTMB will identify the activities DTMB can perform within our existing resources, then assess the additional resources and potential funding required to scan and remediate Microsoft SQL vulnerabilities based on risk and where appropriate for operational and business needs of the organization.

Finding #6 – Access Controls

DTMB agrees it should recertify privileged database accounts and monitor the accounts database administrators 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 reduces the risk of inappropriate access to State data by ensuring 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 rightsizing the State's Technical Standards and Procedures and developing a set of tailored security control baselines based on the National Institute of Standards and Technology (NIST) control framework to ensure the controls for each information system are appropriate for the information types it processes (anticipated completion 2021). As part of this process, DTMB

has developed a parameterized NIST control framework set (March 2020). DTMB is also reviewing and streamlining the State's Technical Standards and Procedures, and will identify appropriate evidence to confirm DTMB is complying with the new parameterized control framework and the State's Technical Standards and Procedures (anticipated completion 2021). This process will implement the NIST Risk Management Framework.

As part of the State's biennial Internal Control and Evaluation (ICE) process, DTMB is completing System Security Plans (SSP) for the State's general IT support systems and will identify the risks which will be remediated. DTMB will then identify the activities to remediate these risks and assess which activities DTMB can perform within our existing resources and which activities will require additional resources and potential funding.

The alignment of this effort with the upcoming ICE process will reduce rework and enable DTMB's strategic goal of the responsible use of Taxpayer revenue. DTMB will identify applicable controls for the State's general IT support systems and the standard appropriate evidence to confirm DTMB is complying with the new tailored NIST control baseline and the State's Technical Standards and Procedures. The owner of each general IT support system will generate appropriate audit evidence which will be reused for subsequent audits during the period until the next evaluation.

DTMB has also assigned an individual to update DTMB-IT executives regarding information technology audits and progress to reducing risks identified in OAG information technology audit reports.

Prior to the completion of the OAG's audit, DTMB completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational database management improvements via a Lean Process Improvement, similar to Six Sigma (January and February 2020). The Lean Process Improvement (LPI) teams are identifying the resource requirements and activities necessary to implement the improved processes identified in the LPI and to implement further risk reductions. These efforts will improve DTMB's security posture for databases.

DTMB has completed the following activities to improve governance and reduce risks identified in the audit:

Governance Activities:

- DTMB created an email distribution list to improve communication to DBAs across the organization (January 2020).
- DTMB has drafted an organizational approach to develop and maintain common and consistent database practices to improve compliance and security across the organization (July 2020).
- DTMB DBAs completed a survey identifying tools used for database management activities (93% participation) which can be used to promote governance through the standardization of tools and skills training (June 2020).

- DTMB reviewed and documented necessary updates to the State's Enterprise Database Standard 1340.00.060.02 Database Security Standard (June 2020).

Security and Access Control Activities:

Database security configurations:

- DTMB conducted working sessions identifying the process for the technical implementation of database security configuration scanning, with the initial focus on configuring the scanning tool and ensuring the tool can access the database servers (June 2020).

Encryption in transit:

- DTMB developed a script identifying whether encryption-in-transit is enabled for Microsoft SQL databases (November 2019).
- DTMB has drafted initial guidance to configure and enable Microsoft SQL database encryption-at-rest and encryption-in-transit (July 2020).

Vulnerability scanning:

- DTMB has 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 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 has 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 (May 2020).
- DTMB completed a high-level estimate to assess the resources necessary to remediate SQL server vulnerabilities (February 2020).

Privileged accounts:

- DTMB provisioned privileged accounts for DBAs who perform SQL server database administration activities (July 2020).
- DTMB developed guidance to DBAs for requesting a privileged account (July 2020).
- DTMB developed guidance for the use of privileged accounts for SQL server database administration (April 2020).

As part of DTMB's rightsizing of the State's Technical Standards and Procedures, DTMB is reviewing cost effective and operationally efficient means to secure our systems using available cybersecurity capabilities. DTMB's efforts to tailor the NIST baseline will promote DTMB's application of the relevant controls to the appropriate information types.

Even after rightsizing the State's Technical 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 the process is consistently implemented across the organization. DTMB will identify the activities DTMB can perform within our 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 – High-Risk Event Monitoring

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

DTMB reduces the risk by ensuring 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 Technical Standards and Procedures and developing a set of tailored security control baselines based on the National Institute of Standards and Technology (NIST) control framework to ensure the controls for each information system are appropriate for the information types it processes (anticipated completion 2021). As part of this process, DTMB has developed a parameterized NIST control framework set (March 2020). DTMB is also reviewing and streamlining the State's Technical Standards and Procedures, and will identify appropriate evidence to confirm DTMB is complying with the new parameterized control framework and the State's Technical Standards and Procedures (anticipated completion 2021). This process will implement the NIST Risk Management Framework.

As part of the State's biennial Internal Control and Evaluation (ICE) process, DTMB is completing System Security Plans (SSP) for the State's general IT support systems and will identify the risks which will be remediated. DTMB will then identify the activities to remediate these risks and assess which activities DTMB can perform within our existing resources and which activities will require additional resources and potential funding.

The alignment of this effort with the upcoming ICE process will reduce rework and enable DTMB's strategic goal of the responsible use of Taxpayer revenue. DTMB will identify applicable controls for the State's general IT support systems and the standard appropriate evidence to confirm DTMB is complying with the new NIST control baseline and the State's Technical Standards and Procedures. The owner of each general IT support system will generate appropriate audit evidence which will be reused for subsequent audits during the period until the next evaluation.

DTMB has also assigned an individual to update DTMB-IT executives regarding information technology audits and progress to reducing risks identified in OAG information technology audit reports.

Prior to the completion of the OAG's audit, DTMB completed an initial review to identify processes, gaps, and constraints, and mapped new processes to address organizational database management improvements via a Lean Process Improvement, similar to Six Sigma

(January and February 2020). The Lean Process Improvement (LPI) teams are identifying the resource requirements and activities necessary to implement the improved processes identified in the LPI and to implement further risk reductions. These efforts will improve DTMB's security posture for databases.

DTMB has completed the following activities to improve governance and reduce risks identified in the audit:

Governance Activities:

- DTMB created an email distribution list to improve communication to DBAs across the organization (January 2020).
- DTMB has drafted an organizational approach to develop and maintain common and consistent database practices to improve compliance and security across the organization (July 2020).
- DTMB DBAs completed a survey identifying tools used for database management activities (93% participation) which can be used to promote governance through the standardization of tools and skills training (June 2020).
- DTMB reviewed and documented necessary updates to the State's Enterprise Database Standard 1340.00.060.02 Database Security Standard (June 2020).

Security and Access Control Activities:

Database security configurations:

- DTMB conducted working sessions identifying the process for the technical implementation of database security configuration scanning, with the initial focus on configuring the scanning tool and ensuring the tool can access the database servers (June 2020).

Encryption in transit:

- DTMB developed a script identifying whether encryption-in-transit is enabled for Microsoft SQL databases (November 2019).
- DTMB has drafted initial guidance to configure and enable Microsoft SQL database encryption-at-rest and encryption-in-transit (July 2020).

Vulnerability scanning:

- DTMB has 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 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 has 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 (May 2020).
- DTMB completed a high-level estimate to assess the resources necessary to remediate SQL server vulnerabilities (February 2020).

Privileged accounts:

- DTMB provisioned privileged accounts for DBAs who perform SQL server database administration activities (July 2020).
- DTMB developed guidance to DBAs for requesting a privileged account (July 2020).
- DTMB developed guidance for the use of privileged accounts for SQL server database administration (April 2020).

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.