Office of the Auditor General
Performance Audit Report

Statewide Windows Active Directory Environments

Department of Technology, Management, and Budget and Other Agencies

July 2017

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

071-0564-16

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

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit
Statewide Windows Active Directory Environments
Department of Technology, Management, and Budget (DTMB) and Other Agencies

Report Number:
071-0564-16

Released:
July 2017

Active Directory is Microsoft's directory service product that contains information for managing users and resources in a computer network. Active Directory provides the means to centrally manage network users, groups, computers, servers, printers, network shares, and system information while enforcing the State's security standards. As of April 2016, the State's executive branch Active Directory environments were composed of 23 forests (the outmost boundary) and 27 domains (a portion within a forest consisting of select groups of users, computers, etc.). DTMB Infrastructure and Operations has the primary responsibility for administering and securing the State's executive branch Active Directory environments.

Audit Objective	Conclusion
Objective #1: To assess the sufficiency of the State's governance over its Active Directory environments.	Not sufficient

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB and a separate State agency had not fully established and implemented sufficient governance over the Active Directory environments. Establishing and implementing governance would help DTMB address the root cause of the findings reported in Objectives #2 and #3 (Finding #1).	X		Agrees
DTMB had not fully established and implemented approved baseline configurations to ensure that the State's domain controllers are securely configured. These configurations help to ensure that all domain controllers are properly configured to enforce the State's security requirements (Finding #2).	X		Agrees
DTMB and a separate State agency did not monitor all high risk Active Directory security events and did not always properly secure the event logs. Without monitoring, DTMB cannot ensure that all privileged activities are authorized and that security violations and other unauthorized activities are detected in a timely manner (Finding #3).	X		Agrees

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB, in conjunction with State agencies, should assess the feasibility and value of consolidating executive branch Active Directory forests and domains. Performing such an assessment would help DTMB determine if a consolidated Active Directory would result in a more efficient, cost-effective, and secure environment. Also, the State should implement the assessment results if the changes would have a positive impact (Finding #4).		X	Agrees
DTMB did not maintain a complete and accurate record of Active Directory information in the Configuration Management Database to help ensure the availability of information necessary for business decisions and the security of IT resources (Finding #5).		X	Agrees
DTMB did not monitor a separate State agency and a vendor responsible for securing certain Active Directory environments to ensure compliance with State standards (Finding #6).		X	Agrees
DTMB needs to improve its training program to help ensure that administrators obtain the knowledge and skills to effectively administer and secure Active Directory (Finding #7).		X	Agrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of the State's efforts to implement security and access controls over its Active Directory environments.	Not effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB and a separate State agency did not fully ensure that the State's Active Directory domains were configured in accordance with best practices. Properly configured domain controller operating systems reduce the risk of unauthorized access to the State's information systems and data, thereby protecting them from unauthorized modification, loss, or disclosure (Finding #8).	X		Agrees
DTMB and a separate State agency did not fully establish effective controls over users and groups with administrative access to the State's domain controllers to ensure the security of the domain controllers and Active Directory (Finding #9).	X		Agrees
DTMB and a separate State agency had not fully established effective controls over the management of non-user accounts to reduce the risk of unauthorized access (Finding #10).	X		Agrees
DTMB and a separate State agency did not ensure that all user accounts were configured to enforce the State's password requirements (Finding #11).	X		Agrees

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB and a separate State agency did not ensure that updated antivirus software was fully deployed. Consequently, the domain controllers may be more vulnerable to attack by malicious code such as viruses and spyware (Finding #12).	X		Agrees
DTMB did not patch all domain controller operating systems in a timely manner to enhance security and help protect the domain controllers from attack or intrusion (Finding #13).	X		Agrees

Audit Objective	Conclusion
Objective #3: To evaluate the effectiveness of the State's controls to add, modify, and delete Active Directory accounts.	Not effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB and a separate State agency, in conjunction with State agencies, did not establish effective user account management controls to ensure that all Active Directory accounts were properly authorized and that all accounts not requiring access were disabled or deleted in a timely manner (Finding #14).	X		Agrees
DTMB and a separate State agency, in conjunction with State agencies, did not periodically recertify user accounts for all Active Directory domains or did not sufficiently document the results and corresponding follow-up actions of recertification reviews. Periodic recertification of Active Directory accounts helps ensure that all accounts are authorized and have an appropriate level of access (Finding #15).	X		Agrees
DTMB needs to clarify and update its record retention and disposal schedule for DTMB-161 forms and MiID records to ensure that all account management activities are properly authorized and documented (Finding #16).		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

This Page Left Intentionally Blank

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

July 25, 2017

Mr. Brom Stibitz, Interim Director
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Stibitz:

I am pleased to provide this performance audit report on the Statewide Windows Active Directory Environments, Department of Technology, Management, and Budget and Other Agencies.

We organize our findings and observations by audit objective. Your agency provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and submit it within 60 days of the date above to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

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

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

STATEWIDE WINDOWS ACTIVE DIRECTORY ENVIRONMENTS

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

GOVERNANCE OVER ACTIVE DIRECTORY ENVIRONMENTS

BACKGROUND

IT governance is the leadership, structures, and processes that enable an organization to achieve its strategies and objectives. According to the IT Governance Institute* (ITGI), IT management should focus on making the organization more effective, increasing operational efficiencies and decreasing costs, and managing risks associated with security*, reliability, and compliance.

The Department of Technology, Management, and Budget's (DTMB's) Michigan Cyber Security, Design and Delivery, and Technical Services units have primary responsibility for governance over the State's Active Directory environments. Active Directory is Microsoft's directory service* product that contains information for managing users and resources in a computer network.

Michigan Cyber Security is responsible for establishing and enforcing enterprise-wide security policies. Design and Delivery and Technical Services are responsible for implementing the State's security policies through the design and administration of Active Directory. In addition, a separate State agency is responsible for the administration and security of its Active Directory environment.

AUDIT OBJECTIVE

To assess the sufficiency of the State's governance over its Active Directory environments.

CONCLUSION

Not sufficient.

FACTORS IMPACTING CONCLUSION

- Three material conditions* related to establishing sufficient governance over the Active Directory environments, establishing and implementing baseline configurations for the State's domain controllers*, and monitoring high risk Active Directory security events and properly securing the event logs (Findings #1 through #3).

- Four reportable conditions* related to assessing the feasibility of consolidating the executive branch Active Directory forests* and domains*, maintaining a complete and accurate record of Active Directory information in the Configuration Management Database* (CMDB), ensuring that the separate State agency and a vendor responsible for securing Active Directory environments follow State standards, and improving DTMB's training program (Findings #4 through #7).

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

- Deficiencies in the design of governance controls are the root cause for the material and reportable conditions reported in Objectives #2 and #3.

- DTMB has issued some operational procedures related to Active Directory administration.

- DTMB has implemented or begun implementing automated tools for managing and monitoring security and access.

FINDING #1

Sufficient governance needed to protect Active Directory.

DTMB and a separate State agency had not fully established and implemented sufficient governance over Active Directory environments. Establishing and implementing governance would help DTMB address the root cause of the findings reported in Objectives #2 and #3.

According to ITGI, effective governance includes:

- Assignment of roles, responsibilities, authority, and accountability.
- Development and maintenance of policies, standards, and procedures.
- Periodic risk assessments.
- Adequate, effective, and tested controls for people, processes, and technology.
- Processes to monitor security.

DTMB had not:

Roles and responsibilities for administration and security were not adequately defined.

a. Adequately defined roles and responsibilities for Active Directory administration and security.

   The National Institute of Standards and Technology* (NIST) states that the responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be explicitly defined. For example, DTMB should:

   (1) Assign overall responsibility for Active Directory security.

   (2) Formalize State agency responsibilities for account management.

b. Fully developed procedures and standards relevant to the secure administration of Active Directory.

   DTMB Administrative Guide policy 1340 adopted NIST Special Publication 800-53 as the minimum security controls for the State's information systems. The policy requires groups* responsible for administering information systems to develop and adopt formal, documented procedures to implement and monitor security controls.

   DTMB and the separate State agency had developed some operating procedures for actions such as

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

creating, modifying, and removing user accounts; adding members to global security groups; resetting passwords; and developing server* patch management processes. However, DTMB needs to:

Procedures and standards should be more fully developed.

(1) Fully develop procedures and standards to implement policy 1340 and industry best practices such as:

(a) Appropriate use of administrative level privileges.

(b) User account recertification.

(c) Authorization, management, and recertification of non-user accounts.

(d) Segregation of duties* over group policy* object management.

(e) Granting privileged access* and monitoring of privileged activity.

(f) Virus protection management.

(2) Assess whether it should align Technical Standard 1340.00.080.01, Identification and Authentication Standard, with industry best practices.

The Standard did not:

(a) Meet industry best practices for 4 of 6 password policy configurations*.

(b) Distinguish between password policy for privileged accounts* and regular end-user accounts. Privileged accounts include administrative, service, application, and other non-user accounts.

Although DTMB's password policy may be reasonable for regular end-user accounts, it is not adequate for privileged accounts.

c. Performed required risk assessments* and fully developed risk mitigation plans for its Active Directory environments.

DTMB Technical Standard 1340.00.150.01 states that a risk assessment should be performed at least annually or when a significant change to the system occurs. Also, DTMB Technical Standard 1360.00.10 states that these assessments must be documented, integrated, and

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

practiced using the DTMB-0170 Project Security Plan and Assessment form. Specifically, DTMB had not:

(1) Completed a DTMB-0170 form for Active Directory and had not finalized the DTMB-0170 form for MiID*, its Active Directory user provisioning tool.

Vulnerabilities need to be addressed.

(2) Prepared formal risk mitigation plans to remediate vulnerabilities* identified during its biennial Active Directory risk assessment.

As part of its contract with the State, Microsoft performs a biennial risk assessment of the State's Active Directory security. DTMB informed us that it remediated issues noted in the risk assessment as needed and that formal remediation plans were not developed. However, we noted that many issues identified by our audit, such as the lack of monitoring of administrative accounts and improperly configuring password parameters and security options, were also reported in the risk assessment.

d. Fully established controls to ensure that all changes to the Active Directory environment are authorized and appropriately documented.

State of Michigan (SOM) Technical Standard 1345.00.80 requires that an Enterprise Architecture Solution Assessment (EASA) be submitted, reviewed, and approved for all State IT projects. Also, SOM Technical Procedure 1340.00.060.04.01 requires that a request for change (RFC) be submitted for all changes in the IT life cycle. Specifically, DTMB did not:

(1) Maintain plans and authorization records for all changes to the Active Directory environment.

EASAs or RFCs did not exist for:

(a) 10 (59%) of 17 judgmentally selected decommissioned domains. A decommissioned domain is one that has been removed from service.

(b) 1 (33%) of 3 judgmentally selected domain creations. Creating a domain is the process of adding a domain into service.

(c) 2 (40%) of 5 judgmentally selected trust creations. Creating a trust is the process of establishing a relationship between domains that allows accounts in one domain to access resources in another domain.

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

(2) Implement processes to periodically evaluate trusts to ensure that the trusts are still required, that the trusts are the correct type, and that the security controls are sufficient.

As a result, DTMB had not removed 11 stale trusts. A trust becomes stale when one of the domains in the trust relationship is no longer active.

We consider this finding a material condition because, without effective oversight, DTMB has not established defined, repeatable processes to ensure that the State's Active Directory environments are and remain properly secured. In addition, a lack of formal processes to remediate identified risks increases the likelihood that known vulnerabilities will possibly be exploited.

RECOMMENDATION

We recommend that DTMB and the separate State agency fully establish and implement sufficient governance over Active Directory environments.

AGENCY PRELIMINARY RESPONSE

DTMB and the separate State agency provided us with the following response:

DTMB and the separate State agency agree that governance needs to be fully established and implemented. DTMB and the separate State agency have initiated a review of enterprise IT standards and are including all stakeholders in the drafting and review process. The goal of this review is to further enhance and clarify enterprise IT standards. Efforts are also underway to update the DTMB-170 in Lockpath for both AD and the MiID Automated Account Provisioning Tool. Additionally, the process of conducting risk assessments has been enhanced through assignment of issue resolution responsibility to individuals, and regular meetings are being held to ensure timely response. Finally, documentation surrounding the creation, modification, and decommissioning of legacy Active Directory environments is being created where it does not already exist and revised where existing documentation does not adhere to current standards.

FINDING #2

Need to establish and implement baseline configurations.

DTMB had not fully established and implemented approved baseline configurations* to ensure that the State's domain controllers are securely configured. Implementing standard baseline configurations would help DTMB reduce the risk that a malicious user could exploit weaknesses in the domain controllers' configurations.

Baseline configurations are important because they ensure that all domain controllers are properly configured to enforce the State's security requirements.

Specifically, DTMB did not:

a. Approve standard baseline configurations for securing the domain controller operating systems* and did not develop security configuration checklists.

   SOM Technical Standard 1340.00.060.01 requires administrators* to implement baseline configurations using a security configuration checklist that reflects the most restrictive mode consistent with operational requirements.

   Informally, the administrators used Center for Internet Security* (CIS) benchmarks or Microsoft best practices as a basis for securing the domain controllers.

b. Establish a formal process to review and update baseline configurations of the domain controllers.

   According to SOM Technical Standard 1340.00.060.01, baseline configurations should be reviewed and updated:

   - According to the system's configuration management* program or at least every 90 days.
   - When required because of a major system change or upgrade.
   - As an integral part of IT component installations and upgrades.

Periodic review needed to ensure compliance with baseline configuration standard.

Although the administrator for 1 (14%) of 7 administrative groups informed us that he compared and modified a domain's current configuration to agree with CIS and Microsoft best practices whenever new versions of the best practices were released, DTMB had not established a formal review process.

c. Establish a process to routinely audit the domain controllers' security configuration settings to ensure that

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

the settings are in compliance with an approved baseline.

SOM Technical Standard 1340.00.060.01 requires that DTMB monitor and control changes to the configuration settings in accordance with organizational policies and procedures. Implementing an audit process will help DTMB reduce the risk that insecure security configuration settings go undetected.

During our fieldwork, DTMB updated SOM Technical Standard 1345.00.13 to adopt CIS as the State's primary security standard for server security configurations.

We consider this finding a material condition because administrators used different standards for securing domain controllers and, consequently, the domain controllers were not secured in accordance with DTMB standards and industry best practices.

RECOMMENDATION

We recommend that DTMB fully establish and implement approved baseline configurations for the State's domain controllers.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the importance of establishing approved baseline configurations for the State's domain controllers. In accordance with SOM Technical Standard 1345.00.13, DTMB is working to formally document all existing standard baseline configurations as well as the schedule to review and recertify approved and documented standard baseline configurations of the State's domain controllers. DTMB will establish a process for the routine audit of security configuration settings of domain controllers to ensure the settings are compliant with approved baselines.

FINDING #3

Improvements needed in monitoring security events and securing event logs.

DTMB and a separate State agency did not monitor all high risk Active Directory security events and did not always properly secure the event logs.

A log is a record of the events occurring within an organization's systems and networks. Log management is essential to ensure that security records are stored in sufficient detail for an appropriate period of time. Log management includes controls over log generation, transmission, analysis, storage, and disposal.

SOM Technical Standard 1340.00.040.01 requires information systems to log certain categories of security events and requires agencies to monitor the event logs on at least a weekly basis.

Our review of the State's monitoring processes for 25 domains disclosed:

Event logs not always monitored.

a. DTMB did not monitor event logs for all domains. According to NIST, routine monitoring is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems.

   DTMB informed us that these events were being forwarded to external log collection systems; however, the log systems were not in production and procedures had not been established to review the logs and follow up on suspicious activity. Without a well-developed process for monitoring events, the value in maintaining log data is significantly reduced.

b. DTMB and the separate State agency did not:

   (1) Monitor all security events.

   Because of the confidentiality of this monitoring, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB and the separate State agency management.

   The high risk events were not monitored because DTMB had not performed a comprehensive review of Active Directory events to determine which events should be monitored in accordance with DTMB standards.

   (2) Establish an appropriate segregation of duties by restricting administrator access to the log server and by implementing independent monitoring of privileged administrator activity for all domains.

   Although administrators require read access to log files to monitor for operational problems and other non-security concerns, SOM Technical Standard 1340.00.040.01 states that administrators must not

have the ability to modify and delete log entries. In addition, NIST states that organizations should establish segregation of duties by having someone other than the administrator review the logs to provide accountability for the administrator's actions, including confirming that logging is enabled.

(3) Develop formal event response procedures for all domains.

To ensure that anomalies and suspicious activity are properly addressed, procedures should be developed to identify the actions which should be taken when specific events are identified. DTMB informed us that administrators used professional judgment to determine the appropriate response to security events.

We consider this finding a material condition because, without effective monitoring, DTMB and the separate State agency cannot ensure that all privileged activities are authorized and that security violations and other unauthorized activities are detected in a timely manner.

RECOMMENDATION

We recommend that DTMB and the separate State agency monitor all high risk Active Directory security events and establish effective processes for managing the event logs.

AGENCY PRELIMINARY RESPONSE

DTMB and the separate State agency provided us with the following response:

DTMB and the separate State agency agree with the importance of monitoring Active Directory security events. DTMB and the separate State agency are working to define the list of high-risk events that should be monitored. Additionally, DTMB and the separate State agency will establish effective processes for monitoring event logs, covering the topics of retention, separation of duties, non-repudiation, and event response.

FINDING #4

Active Directory consolidation may improve security.

DTMB, in conjunction with State agencies, should assess the feasibility and value of consolidating executive branch Active Directory forests and domains. Performing such an assessment would help DTMB determine if a consolidated Active Directory would result in a more efficient, cost-effective, and secure environment. Also, the State should implement the assessment results if the changes would have a positive impact.

A forest is the outermost security boundary and defines the scope of authority for administrators. As such, administrative activities to secure the Active Directory must be performed for each forest.

According to Microsoft best practices, organizations should minimize the number of Active Directory forests to reduce the administrative costs of operating separate directories and facilitate resource sharing. Microsoft and other industry experts recommend that organizations merge their autonomous directories into a single forest unless legal or security requirements require additional forests.

Active Directory consolidation could result in several benefits. For example, in its 2008 submission to the National Association of State Chief Information Officers (NASCIO), the State of Missouri reported that it had realized the following benefits from consolidating the Active Directory and e-mail systems of 14 state agencies:

- Cost savings and avoidance of administrative costs.
- Reduction in infrastructure.
- Improvements in incident response time.
- Enhanced security and reduced exposure.
- Simplification to business continuity and disaster recovery.

DTMB informed us that, over the past 10 years, it has consolidated approximately 50 to 60 directories into the current Active Directory structure. As of April 2016, the executive branch Active Directory environment included 23 forests and 27 domains administered by 7 administrative groups. During our audit fieldwork, DTMB informed us that it was in the process of eliminating 1 forest and 4 domains.

The number of Active Directory environments exceeds Microsoft recommendations.

Based on Microsoft best practices for the design and management of Active Directory, DTMB's assessment should identify an optimal Active Directory design that:

a. Identifies and documents all operational and legal requirements requiring a separate forest or independent administration.

   DTMB and several State agencies informed us that business and regulatory requirements prohibited the

consolidation of their agencies' forests and domains into a single Active Directory forest. However, DTMB did not require the agencies to develop business cases for maintaining a separate environment and had not established formal review and approval processes.

b. Separates and, where possible, reduces levels of administrative access.

   Microsoft recommends separating administrative responsibilities between domain administrators who are responsible for the configuration and delivery of directory service and data administrators who are responsible for managing users and computers.

   In addition, Microsoft recommends taking steps to secure the enterprise administrator role. For example, Microsoft suggests granting enterprise administrator access only when the access is required to perform enterprise administrator tasks.

   For the 25 domains reviewed, DTMB had approximately 162 administrators, 93 domain administrators, and 33 enterprise administrators. Forty-six administrators were in 2 administrative groups and 33 administrators were in all 3 groups.

c. Standardizes Active Directory administration through the use of common policies, standards, procedures, and tools.

   Because each group of administrators functions independently, Active Directory is managed using multiple administrative processes and tools. Standard processes and tools will improve the consistency and efficiency* of administrative functions and the effectiveness* of compliance monitoring.

Challenges may be encountered when consolidating Active Directory environments.

Our research identified several challenges that DTMB may encounter when consolidating Active Directory. For example:

- Active Directory consolidation can be contentious because of real or perceived loss of control by agencies and administrators.
- The benefits of Active Directory consolidation may be qualitative, such as enhanced administrator productivity and overall security, rather than quantitative.
- Active Directory consolidation is complex because of differences in the design of existing Active Directory environments.

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

However, DTMB has the executive authority to overcome these barriers. Executive Order No. 2001-3 requires DTMB, under the guidance and direction of the State's chief information officer, to reengineer the State's IT infrastructure to achieve the use of common technology across the executive branch. In addition, the executive order requires DTMB to identify best practices from executive branch agencies and other public and private sector entities and develop and implement processes to replicate IT best practices and standards throughout the executive branch.

Consolidating the executive branch Active Directory environments aligns with DTMB's IT principles and priorities. To be successful, consolidation activities require collaboration across DTMB's organization, including the Office of Enterprise Architecture, Michigan Cyber Security, and Infrastructure and Operations Division, and input from State agencies to identify unique business and security requirements that would impact the overall design.

RECOMMENDATIONS

We recommend that DTMB, in conjunction with State agencies, assess the feasibility and value of consolidating executive branch Active Directory forests and domains.

We also recommend that the State implement the assessment results if the changes would have a positive impact.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB and State departments and agencies agree with the value of Active Directory consolidation. The process for assessing the forest and domain environment has been ongoing since the implementation of the M1 Project, where enterprise IT operations were consolidated into a single support center. The result of this project was the receipt of the NASCIO award in 2005 for the submission titled: "Implementation of Consolidated IT Services" in the category of Digital Government Management. It was with this award that the State of Michigan paved the way for states like Missouri to pursue proven efficiencies in operation and cost, by centralizing not only enterprise IT operations but also directory services. Additionally, following its consolidation of more than 65% of its directory services, DTMB recognizes that there is room for improvement through further consolidation of Active Directory services and will continue to assess and implement additional consolidation as appropriate. In conclusion, during the audit process, DTMB completed consolidation of 6 (24%) of 25 domains that were the focus of this audit. In all cases, the efforts to consolidate these domains was underway prior to the start of the audit.

FINDING #5

Improvements to the Configuration Management Database needed to ensure availability of information.

DTMB did not maintain a complete and accurate record of Active Directory information in the Configuration Management Database (CMDB) to help ensure the availability of information necessary for business decisions and the security of IT resources.

DTMB Technical Standard 1345.00.50 requires that all server hardware, operating systems, and applications be fully documented in the CMDB.

Our review of selected information in the CMDB as of October 2016 disclosed:

a. The CMDB did not contain complete information. For example, the CMDB did not include:

   (1) 8 (30%) of the State's 27 operational domains.

   (2) 18 (18%) of the 100 domain controllers supporting these domains.

CMDB not complete for 8 (30%) and 18 (18%) operational domains and domain controllers, respectively.

b. The CMDB did not contain accurate information. For example:

   (1) 5 (19%) of 27 operational domains did not identify the correct domain name.

   (2) 5 operational domain controllers were joined to a decommissioned domain.

   (3) 3 (16%) of 19 domain controllers did not identify the correct operating system version.

   (4) 10 (12%) of 82 domain controllers did not identify the correct operational status.

   (5) 25 (30%) of 82 domain controllers did not identify the correct domain membership.

CMDB not accurate in relation to domain name (19%), domain controller operating system (16%), and domain membership (30%)

DTMB informed us that the CMDB contained incomplete and inaccurate information because manual processes to update the CMDB were not always performed properly.

RECOMMENDATION

We recommend that DTMB maintain a complete and accurate record of Active Directory information in the CMDB.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with importance of maintaining a complete and accurate record of Active Directory information in the CMDB. To maintain the most accurate information available, DTMB is working to ensure that the CMDB business processes are as efficient and automated as possible.

FINDING #6

Monitoring needed to ensure the separate State agency and a vendor follow State standards.

DTMB did not monitor the separate State agency and a vendor responsible for securing certain Active Directory environments to ensure compliance with State standards. Monitoring helps DTMB ensure that all of the State's Active Directory environments are secure and that controls are properly designed and implemented in accordance with State security standards.

According to Control Objectives for Information and Related Technology* (COBIT), organizations should ensure that enterprise requirements are outlined within contracts or service level agreements. COBIT identifies security management and monitoring of performance as critical requirements to be included within these agreements. Also, COBIT states that organizations should plan for independent audit and assurance of these processes to confirm that the agreed-upon requirements are adequately addressed.

DTMB Technical Standard 1340.00.03 requires third parties to follow State security standards by use of contracts and security agreements. The Standard also requires that third parties be monitored and audited for compliance.

We noted:

a. DTMB had not established a formal agreement with the separate State agency responsible for Active Directory security and administration. As a result, DTMB did not have monitoring processes in place to ensure that the agency followed State standards. Examples of items that the agreement should address include:

   - Roles and responsibilities of both parties.
   - Description of the Active Directory environment.
   - Compliance with State policies, standards, and procedures.
   - Remedies for instances in which compliance with State policies, standards, and procedures cannot be achieved.

b. DTMB did not monitor one vendor who shares responsibility for securing and administering Active Directory. DTMB's contract with the vendor requires that the vendor adhere to State standards and grants DTMB the right to audit the vendor's compliance with the contract. DTMB should implement a formalized process to verify that Active Directory controls are implemented in compliance with State standards.

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

RECOMMENDATION

We recommend that DTMB monitor the separate State agency and a vendor responsible for securing certain Active Directory environments to ensure compliance with State standards.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB and the separate State agency agree that monitoring directories managed by groups outside DTMB is critical to the security of the enterprise Active Directory environments. DTMB is working with all stakeholders to establish a documented and manageable process to ensure that directories managed by groups outside DTMB are managed in accordance with State standards.

FINDING #7

Training program improvements needed.

DTMB needs to improve its training program to help ensure that administrators obtain the knowledge and skills to effectively administer and secure Active Directory.

According to COBIT, training programs should be developed and delivered to ensure that employees have the knowledge and skills necessary to achieve enterprise goals, including security requirements. SOM Technical Standard 1340.00.030.01 states that role-based security training should be provided to personnel with security roles and responsibilities. The Standard also requires that individual training records be retained and the effectiveness of the training program be evaluated on a yearly basis.

Our review of administrators' training programs for each of the five divisions responsible for managing Active Directory administrators disclosed that DTMB had not:

a. Provided training to administrators in 1 (20%) of the 5 divisions. DTMB informed us that training was not provided because of the administrators' knowledge of the Windows operating system. However, because technology changes frequently, DTMB should ensure that all administrators receive periodic specialized security training.

b. Evaluated the training effectiveness for 4 (80%) of the 5 divisions. According to NIST, evaluating training effectiveness is a vital step to ensuring that training is cost effective and satisfies the organization's needs.

c. Maintained formal training records for 2 (40%) of the 5 divisions. Maintaining records provides evidence that Active Directory administrators have received training in accordance with DTMB standards.

RECOMMENDATION

We recommend that DTMB improve its training program to help ensure that administrators obtain the knowledge and skills to effectively administer and secure Active Directory.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the need for improvements in the documentation of existing Active Directory administrator training programs. All five divisions are working to ensure that their Active Directory training programs are standardized to allow for consistent administration of Statewide Active Directory environments and that they provide Active Directory-specific security training, which is regularly evaluated for effectiveness and formally documented in a training records database.

IMPLEMENTATION OF SECURITY AND ACCESS CONTROLS

BACKGROUND

Active Directory is the foundation of the State's IT infrastructure and is a key component in securing the State's IT assets. Active Directory controls access to the State's network, applications, and data.

Specifically, Active Directory:

- Contains accounts, groups, and passwords for user authentication and authorization.
- Stores and protects administrative accounts, security groups, and passwords.
- Allows delegation of administrative authority for vital aspects of IT management such as the ability to reset passwords and grant access to resources.
- Stores and transmits security policies for other servers, computers, and mobile devices.

Ensuring that the State's domain controller servers are securely configured is a key factor in ensuring the security of the State's Active Directory environments.

Access controls* limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss, and disclosure.

AUDIT OBJECTIVE

To assess the effectiveness of the State's efforts to implement security and access controls over its Active Directory environments.

CONCLUSION

Not effective.

FACTORS IMPACTING CONCLUSION

- Six material conditions related to domain configurations, controls over administrative access, non-user account management, user account password parameters, antivirus protection, and timely patching of domain controllers (Findings #8 through #13).
- DTMB and a separate State agency implemented some security configurations in accordance with State policy and industry best practices.

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

FINDING #8

Improvements in domain configurations needed to protect Active Directory.

DTMB and a separate State agency did not fully ensure that the State's Active Directory domains were configured in accordance with best practices. Properly configured domain controller operating systems reduce the risk of unauthorized access to the State's information systems and data, thereby protecting them from unauthorized modification, loss, or disclosure.

According to NIST, the first step in securing a server is to secure the underlying operating system. DTMB Administrative Guide policy 1340 establishes access and security controls required for the State's information systems.

We reviewed domain controller operating system configurations for compliance with DTMB policy and industry best practices for 25 domains. Operating system manufacturers provide recommendations on how to secure their operating systems to reduce the risks of unauthorized access. We noted:

Configurations deviated from DTMB policy and industry best practices for 25 domains.

a. Deviations from DTMB policy and industry best practices for 6 key security configurations.

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

b. Improvements needed to ensure that only authorized services are enabled and that services are properly configured.

   For example, DTMB had not documented the services authorized to be installed and running on the State's domain controllers.

   Unauthorized services increase the risk of system attack. Because services often run with increased privileges, compromising a service could allow an unauthorized individual to obtain system level privileges and open the system to a variety of attacks.

This finding represents a material condition because the number of domains and configurations with exceptions points to a systemic problem within DTMB and the separate State agency.

RECOMMENDATION

We recommend that DTMB and the separate State agency fully ensure that the State's Active Directory domains are configured in accordance with best practices.

AGENCY PRELIMINARY RESPONSE

DTMB and the separate State agency provided us with the following response:

DTMB and the separate State agency agree with the recommendation to fully ensure compliance with adopted configuration baselines. In addition to continuing the use of approved baseline configurations, DTMB and the separate State agency will implement scheduled compliance checks (using the highest level of automation feasible) of its Statewide Active Directory environments to ensure ongoing adherence to documented and adopted configuration best practices.

FINDING #9

Improved controls over administrative access would help reduce the risk of unauthorized access.

DTMB and a separate State agency did not fully establish effective controls over users and groups with administrative access to the State's domain controllers to ensure the security of the domain controllers and Active Directory. Unauthorized or unknowledgeable individuals with administrator privileges could maliciously or accidentally cause harm if they copy or delete confidential data, spread viruses, or disable the network.

According to Microsoft, there are two primary kinds of privileged attackers that organizations should guard against:

- Malicious individuals who obtain administrative-level access to domain controllers could breach the security of an entire network. These individuals may be unauthorized users who obtained administrative passwords or legitimate administrators who are coerced or disgruntled.

- Users who are granted administrative access. These individuals might inadvertently cause problems because they fail to understand the ramifications of configuration changes.

Users and groups with administrative access did not meet Microsoft best practices and State policies and technical standards.

For 25 domains, we compared the State's controls over users and groups with administrative access to selected Microsoft best practices as well as State policies and technical standards. Our review disclosed:

a. Five aspects related to administrator accounts that deviated from best practices, policies, or standards. Because of the confidentiality of the accounts, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB and the separate State agency management.

b. DTMB did not use advanced authentication tools such as fine-grained password policies or multi-factor authentication for privileged accounts as required by SOM Technical Standard 1340.00.080.01.

c. DTMB granted access that did not enforce the principle of least privilege* and did not ensure an appropriate segregation of duties. Specifically:

   (1) For 10 (40%) of the 25 domains, administrative access to privileged groups was granted to individuals outside of the organization responsible for administering the domain.

   (2) For 3 (12%) of the 25 domains, administrative access functions were delegated to individuals who did not require the access or had departed State employment.

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

In circumstances where other individuals legitimately require administrative access, SOM Technical Procedure 1345.00.06.01 establishes procedures for requesting temporary elevated rights to production servers for a limited period of time with a justified purpose.

d. For 8 domains that utilized the default administrator account within 365 days of our obtaining data for analysis, none of the administrators maintained documentation of authorization to use the default administrator account. To provide a sufficient audit trail, Microsoft best practices recommend documenting who used the account, when and why the account was used, and what was done with the account.

e. DTMB was unable to delete one former employee's administrative accounts. The employee departed from State employment in June 2011. DTMB informed us that it could not delete the accounts because the employee's credentials were hard coded into programming relied on for business operations. DTMB should rewrite the programs and replace the employee's credentials to comply with the State's account management and identification and authentication standards.

This finding represents a material condition because of the numerous exceptions related to privileged users and privileged accounts both individually and collectively. Privileged accounts are the most powerful and, if compromised, could create a security risk.

RECOMMENDATION

We recommend that DTMB and the separate State agency fully establish effective controls over users and groups with administrative access.

AGENCY PRELIMINARY RESPONSE

DTMB and the separate State agency provided us with the following response:

DTMB and the separate State agency agree with the need to establish controls over users and groups with administrative access. To that end, in April 2017, DTMB carried out a third-party audit of its largest directory. This audit uncovered zero critical and 12 high-priority issues. To date, remediation efforts by DTMB have reduced the number of high-priority issues to two, on which remediation continues. DTMB and the separate State agency are planning to conduct similar third-party audits of other Statewide Active Directory environments and make changes recommended by those audits. Additionally, DTMB and the separate State agency are reviewing existing policies, standards, and procedures with the intent of implementing any identified changes that are necessary. Review topics include

privileged access, administrative workstations, separation of duties, just in time access and other pertinent areas. A report of the review findings will be produced and a plan for implementation will be drafted.

FINDING #10

Improved non-user account management needed to reduce the risk of unauthorized access.

DTMB and a separate State agency had not fully established effective controls over the management of non-user accounts to reduce the risk of unauthorized access.

Non-user accounts are not intended to be controlled directly by a person or a group. Examples of non-user accounts include service, application, and other shared or generic accounts such as training accounts.

Malicious users often target non-user accounts because the accounts have passwords that are shared, do not expire, or cannot be changed. In addition, non-user accounts have privileged access that allows the account to interact with the operating system or access applications and data.

We reviewed non-user accounts on 25 domains. For some audit procedures, we were unable to test all 25 domains. DTMB and the separate State agency did not:

Recertification of non-user accounts needed.

a. Establish processes to periodically recertify non-user accounts.

   Recertification would help to ensure that the accounts are still required and are being used for only authorized purposes.

b. Establish processes for changing non-user account passwords, where possible.

   Poor application design or other operational risks may prevent administrators from changing the account's password.

c. Limit the ability of non-user accounts to access only specific servers for 21 (95%) of 22 domains tested.

   Restricting accounts to specific servers helps limit potential damage if the account is compromised.

d. Grant privileges to non-user accounts based on the principle of least privilege for 13 (57%) of 23 domains tested.

e. Ensure that all non-user accounts required a password for 4 (16%) of 25 domains tested.

f. Configure non-user account properties to prevent a malicious user from logging in with the account and changing the account's password, where appropriate, for 20 (91%) of 22 domains tested.

   One administrator informed us that, for some accounts, business requirements require the account owner to log in with the account to change the account password.

g. Retain documentation of non-user account authorization.

   DTMB informed us that account owners were responsible for retaining documentation of the account's authorization. However, neither DTMB nor the account owner could provide documentation for 16 judgmentally selected accounts on 2 domains. DTMB informed us that documentation did not always exist because the accounts were established prior to the implementation of DTMB's current account management process.

We consider this a material condition because of the lack of established processes and the number of exceptions, collectively, related to non-user account management. This creates an increased risk that accounts with privileged access to the State's data and resources could be compromised.

RECOMMENDATION

We recommend that DTMB and the separate State agency fully establish effective controls over the management of non-user accounts.

AGENCY PRELIMINARY RESPONSE

DTMB and the separate State agency provided us with the following response:

DTMB and the separate State agency agree with the need for improvements in non-user account management. To accomplish the necessary improvements, DTMB and the separate State agency are working to establish a standard for non-user account management as well as policies and procedures that guide implementation of this standard. The standard will address such things as the principle of least privilege, periodic recertification, password change requirements and documentation of authorization for non-user accounts.

FINDING #11

Improved user account password parameters would help reduce the risk of data breaches.

DTMB and a separate State agency did not ensure that all user accounts were configured to enforce the State's password requirements. According to the Verizon 2016 Data Breach Investigations Report, 63% of confirmed data breaches involved weak, default, or stolen passwords.

Users requiring access to the State's network and IT resources must first authenticate to Active Directory by entering a user account and password. Strong password controls reduce the risk that an account could be compromised, thereby allowing an unauthorized user access to the State's information systems and data.

SOM Technical Standard 1340.00.080.01 requires users to change their passwords at least every 90 days. Our review disclosed domains with user accounts that did not meet the State's standard. DTMB informed us that, for some user accounts, business requirements necessitated deviations from the standard. In these circumstances, administrators should obtain a documented State Technical Review Board exception.

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

This finding represents a material condition because weak password parameters increase the likelihood that accounts could be compromised and the number of passwords with exceptions was significant.

RECOMMENDATION

We recommend that DTMB and the separate State agency ensure that all user accounts are configured to enforce the State's password requirements.

AGENCY PRELIMINARY RESPONSE

DTMB and the separate State agency provided us with the following response:

DTMB and the separate State agency agree with the need to adhere to the State's password requirements. In addition to ensuring that password requirements are met, DTMB and the separate State agency will ensure that appropriate exceptions are filed for all accounts that are unable to comply with the published password policy.

FINDING #12

Antivirus protection needed to safeguard against malicious code.

DTMB and a separate State agency did not ensure that updated antivirus software was fully deployed. Consequently, the domain controllers may be more vulnerable to attack by malicious code such as viruses and spyware.

According to NIST, organizations should deploy antivirus software on all servers for which satisfactory antivirus software is available. NIST states that administrators should perform continuous monitoring to confirm that hosts are using the current antivirus software and that the software is configured properly and includes the latest virus signatures.

SOM Technical Standard 1340.00.180.01 requires State organizations to implement malicious code protection mechanisms, such as antivirus software, to detect and eradicate malicious code. The Standard specifies that the mechanism include automatic updates when new releases are available.

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

This finding represents a material condition because antivirus protection is a key control against malicious code.

RECOMMENDATION

We recommend that DTMB and the separate State agency ensure that updated antivirus software is fully deployed.

AGENCY PRELIMINARY RESPONSE

DTMB and the separate State agency provided us with the following response:

DTMB and the separate State agency agree with the recommendation that up-to-date antivirus software be fully deployed. Due to ambiguity within the published standards, DTMB is working to clarify the standards to ensure that no additional audit findings arise. Also, any deviation from this standard will include an approved enterprise exception.

FINDING #13

DTMB did not patch all domain controller operating systems in a timely manner.

Timely patches needed to ensure domain controller security.

Patches correct the security and functionality problems in software that can create vulnerabilities. According to NIST, applying patches is essential to reduce the opportunities for server exploitation. DTMB Technical Standard 1345.00.50 requires that critical patches be applied to domain controllers on a monthly basis.

Timely patching enhances security and helps protect the domain controllers from attack or intrusion.

Because of confidentiality and security related to patching operating systems, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB management.

This finding represents a material condition because patching is a key control in maintaining the availability, confidentiality, and integrity of IT systems. The percentage of controllers without patches demonstrates lack of oversight by DTMB.

RECOMMENDATION

We recommend that DTMB patch all domain controller operating systems in a timely manner.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the need to patch operating systems in a timely manner. During the audit period, DTMB worked to resolve these issues on all identified systems for which an existing exception had not been filed. Additionally, monitoring of patch levels is now in place in all domains where it previously was not.

CONTROLS OVER ACTIVE DIRECTORY ACCOUNTS

BACKGROUND

According to NIST, organizations should ensure effective administration of users' access to maintain system security, including user account management, auditing, and the timely modification or removal of access. User account management includes processes for requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions. In addition, effective user account management includes a periodic recertification of user accounts on a system.

State agencies and other business owners have the primary responsibility to authorize user account access, ensure access is granted based on the principle of least privilege, and provide Active Directory administrators with timely notification when user access is no longer required.

Active Directory administrators are responsible for establishing effective user account management processes and ensuring that user account requests are processed in a timely manner.

AUDIT OBJECTIVE

To evaluate the effectiveness of the State's controls to add, modify, and delete Active Directory accounts.

CONCLUSION

Not effective.

FACTORS IMPACTING CONCLUSION

- Two material conditions related to user account management and user account recertification (Findings #14 and #15).
- One reportable condition related to the record retention and disposal schedule (Finding #16).
- The impact of weaknesses in Active Directory user account management on access to applications and data.
- DTMB's implementation of a user provisioning tool, MiID, for some Active Directory domains.

FINDING #14

More effective user account management needed.

DTMB and a separate State agency, in conjunction with State agencies, did not establish effective user account management controls to ensure that all Active Directory accounts were properly authorized and that all accounts not requiring access were disabled or deleted in a timely manner.

According to NIST, organizations should have processes for requesting, establishing, issuing, and closing user accounts. SOM Technical Standard 1340.00.020.01 requires administrators to establish DTMB-approved and NIST compliant processes to create, enable, modify, disable, and remove accounts.

User account management over the State's Active Directory environments is controlled by seven administrative groups reporting to three DTMB divisions and a separate State agency. For 17 domains administered by one division, requests to add, modify, or delete user access are made by DTMB process owners and State agencies using the DTMB-161 form or the MiID tool. For the other 8 domains, administrators use e-mail or other agency systems to process account requests.

We reviewed controls over the addition, modification, and deletion of Active Directory accounts for the 25 domains. Also, we judgmentally selected and tested documentation for:

- 154 Active Directory accounts in active status. In general, all employees that are authorized to use the State's network have an active account.
- 80 employee departures from the State's Human Resources Management Network* (HRMN).

Our review disclosed that DTMB and a separate State agency, in conjunction with State agencies, did not:

DTMB did not document the authorization to create 98 (64%) of 154 active accounts.

a. Document the authorization to create 98 (64%) of 154 accounts or delete 15 (19%) of 80 accounts in Active Directory.

   SOM Technical Standard 1340.00.020.01 requires account managers to ensure that all user accounts are approved by an authorized requestor.

   DTMB and the separate State agency informed us that authorization documentation did not always exist because the accounts were granted access prior to the implementation of an official account creation and deletion process. Also, for the domains managed by one DTMB division, DTMB informed us that State agencies were responsible for retaining their authorization request forms. However, neither DTMB

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

nor the State agencies were able to provide all of the authorization forms.

b. Disable or delete Active Directory accounts in a timely manner.

SOM Technical Standard 1340.00.020.01 requires account managers to be notified within 24 hours when accounts are no longer required, users are terminated or transferred, or user privileges change. Specifically:

(1) 12 (8%) of 154 Active Directory accounts tested belonged to employees who had departed State employment or no longer required access. The oldest account belonged to an employee who departed State employment in July 2005.

(2) 67 (84%) of 80 departed employees identified in HRMN were not deleted or were not deleted in a timely manner. Specifically:

(a) Accounts for 5 departed employees were not deleted in Active Directory. For 4 accounts, no request to disable the account was on file. For 1 account, DTMB rejected the State agency's request to delete the account because the request was not made by an authorized requestor.

(b) Requests to delete 51 accounts were not made within 24 hours of employee departure.

Number of Days Request Made After Employee Departure	Number of Accounts
2 - 30	23
31 - 365	25
Over 365	3

(c) We were unable to determine the timeliness of deletion requests for 11 accounts because, for 10 accounts, no request was on file and the request was incomplete for 1 account.

c. Establish formal processes to identify and disable inactive accounts in a timely manner.

SOM Technical Standard 1340.00.020.01 requires an information system to automatically disable inactive accounts after 60 days. At the time of our audit, DTMB's requirement was to disable inactive accounts after 120

days. We identified user accounts that appeared to be inactive on 6 judgmentally selected domains:

	Number of Potential Inactive Accounts		
Domain	Over 120	Over 60	Never Interactively Logged In
1	0	0	0
2	1,677	1,943	95
3	7	11	0
4	18	20	1
5	174	225	266
6	4,935	5,729	2,249

The State's processes for identifying and disabling inactive accounts were not effective because administrators primarily relied on State agencies to inform them when a user no longer required access rather than establishing automated processes to identify potential inactive accounts. However, one administrator informed us that he ran a monthly query to identify user accounts that had not changed their password or accessed Active Directory in over 30 days.

Administrators informed us that some active user accounts may mistakenly appear inactive because virtual private networks (VPNs) and other applications that connect with Active Directory may not update the last log-in timestamp. Also, improper password configurations, as noted in Finding #11, may impact the password last set flag.

d. Retain documentation to demonstrate the results of DTMB's weekly match of employee Active Directory accounts with HRMN departure records for the State's largest user account domain.

DTMB was unable to demonstrate that it performed the match because the output logs were overwritten each time the script was run. Upon bringing this matter to management's attention, DTMB informed us that it modified its script to capture the output logs.

e. Maintain a listing of authorized requesters or did not maintain historical records of the listings.

As a result, the State may not be able to demonstrate that access requests were always approved by an authorized source.

We consider this finding a material condition because effective user account management is a key control to ensuring that only authorized users have access to State applications and data. In

addition, error rates indicate that controls were not functioning as intended.

RECOMMENDATION

We recommend that DTMB and the separate State agency, in conjunction with State agencies, establish effective user account management controls.

AGENCY PRELIMINARY RESPONSE

DTMB and the separate State agency provided us with the following response:

DTMB and the separate State agency agree with the need to establish more effective user account management controls. To achieve this outcome, DTMB and the separate State agency are assessing existing policies, standards and procedures; making changes where appropriate; and documenting the entire assessment and resulting recommendations.

FINDING #15

Periodic account recertification needed.

DTMB and a separate State agency, in conjunction with State agencies, did not periodically recertify user accounts for all Active Directory domains or did not sufficiently document the results and corresponding follow-up actions of recertification reviews. Periodic recertification of Active Directory accounts helps ensure that all accounts are authorized and have an appropriate level of access.

Recertification requires managers or other account owners to certify that individuals and accounts under their responsibility still require access to the information system and that the access granted corresponds correctly to the users' responsibilities and the functions they perform. SOM Technical Standard 1340.00.020.01 requires the system owner to ensure that agencies review accounts for compliance every 120 days.

DTMB and a separate State agency did not:

a. Recertify accounts every 120 days for domains managed by 1 administrative group.

   The administrator informed us that:

   (1) The administrative group performed annual recertification for the domains it managed. However, the administrator was unable to provide documentation of the annual recertification process.

   Some State agencies did not respond to requests to recertify user accounts.

   (2) Some State agencies did not respond to requests to recertify Active Directory user accounts. Because DTMB procedures did not require administrators to disable the accounts if the agency did not respond to the recertification request, the recertification process was limited in its effectiveness.

b. Perform formal periodic recertification for domains managed by 6 administrative groups.

This finding represents a material condition because periodic recertification is a key detective control to identify user access that is unauthorized or no longer required based on the individual's current job responsibilities.

RECOMMENDATION

We recommend that DTMB and the separate State agency, in conjunction with State agencies, periodically recertify user accounts for all Active Directory domains and document the results and corresponding follow-up actions of recertification reviews.

AGENCY PRELIMINARY RESPONSE

DTMB and the separate State agency provided us with the following response:

DTMB and the separate State agency agree with the need for periodic recertification of user accounts. DTMB and the separate State agency are working to implement multiple policy, standard, and procedure changes that will facilitate this outcome.

FINDING #16

Improvements needed to record retention and disposal schedule.

DTMB needs to clarify and update its record retention and disposal schedule for DTMB-161 forms and MiID records to ensure that all account management activities are properly authorized and documented.

According to COBIT, management should ensure the traceability and accountability of all information transactions through the capture and retention of source documentation.

DTMB's record retention and disposal schedule requires State agencies to submit a DTMB-161, User ID Network Request Form, to request the creation, modification, and deactivation of Active Directory accounts for all State employees and contractors. The schedule states that DTMB retains these records to document that access was implemented in accordance with the information on the forms. Also, the State's general administrative records retention schedule requires the authorized requestor to retain the access request forms until 5 years after the final de-registration of users who no longer require access to IT resources or until 5 years after completion of an audit of authorized users. DTMB's record retention schedule does not include user account requests processed electronically using the MiID tool. Therefore, DTMB should update its retention schedule to:

a. Establish record retention requirements for user account requests processed electronically using DTMB's MiID tool. DTMB informed us that it has not archived the MiID log; therefore, it should contain a history of all MiID transactions.

b. Specify the retention period for DTMB-161 forms. DTMB did not retain copies of the DTMB-161 forms in accordance with the record retention schedule and, as noted in Finding #14, part a., State agencies did not retain or were unable to locate DTMB-161 forms for all of their employees.

RECOMMENDATION

We recommend that DTMB clarify and update its record retention and disposal schedule for DTMB-161 forms and MiID records.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the need to clarify its record retention and disposal schedule for DTMB-161 forms and MiID records. To this end, DTMB is working with the various stakeholders on these record retention and disposal schedules and updating forms and records as appropriate.

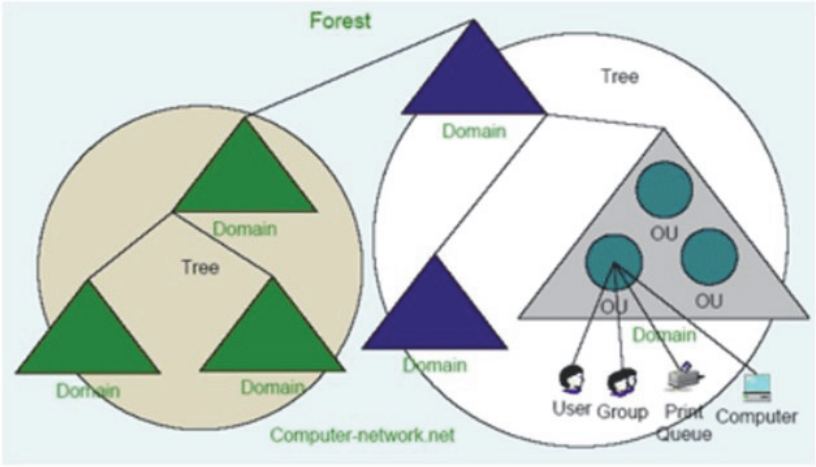
DESCRIPTION

Active Directory is Microsoft's directory service database* for Windows networks. A directory service is a repository of network information to manage users and resources in a network. Active Directory provides the means to centrally manage network users, groups, computers, servers, printers, network shares, and system information while enforcing the State's security standards.

As of April 2016, the State's executive branch Active Directory environments were composed of 23 forests and 27 domains. A forest acts as the outermost security boundary. Domains provide a boundary of policy, such as authentication and domain-level security policies, and replication. Trust relationships are established between domains that allow access by objects in one domain to resources in another. In addition, each domain is further subdivided into organizational units* (OUs). An OU is a container that holds objects such as users, groups, or computers.

A domain controller is a server with Active Directory installed. A domain controller contains the Active Directory database for the domain, plus the configuration container and schema for the forest. The State's executive branch forests contained approximately 100 domain controllers.

The following diagram depicts an example of a generic Active Directory structure:



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

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the program and other records of the State's Windows Active Directory environments. We conducted this performance audit* in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered January 1, 2016 through February 28, 2017. Domain controller configuration data represents a point in time and was obtained between April 27, 2016 and August 23, 2016.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of the State's Windows Active Directory environments and activities in order to establish our audit objectives, scope, and methodology. During our preliminary survey, we:

- Interviewed management and staff responsible for administering and securing Active Directory.
- Reviewed DTMB policies, standards, and procedures for configuring and securing Active Directory.
- Obtained an understanding of the State's Active Directory forests, domains, and trust relationships.
- Compared DTMB policies, standards, and procedures with CIS and Microsoft best practices.

CONFIDENTIAL AND SENSITIVE INFORMATION

Because of security concerns related to certain findings, we summarized our testing results for presentation in the findings. In addition, we did not identify specific domains within the contents of this audit report. We provided the detailed results to DTMB and the separate State agency.

OBJECTIVE #1

To assess the sufficiency of the State's governance over its Active Directory environments.

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

To accomplish this objective, we:

- Determined the sufficiency of DTMB's policies, standards, and procedures for configuring and securing Active Directory.
- Assessed the completeness and accuracy of Windows Active Directory information in the CMDB, which is an inventory of the State's automated systems.
- Reviewed DTMB's risk management activities over the Active Directory environments.
- Evaluated DTMB's processes for configuring domain controllers to industry best practices.
- Reviewed the sufficiency of training provided to Active Directory system administrators.
- Assessed security and controls over Active Directory event logs.

OBJECTIVE #2

To assess the effectiveness of the State's efforts to implement security and access controls over its Active Directory environments.

To accomplish this objective, we:

- Tested selected security configurations for 1 domain controller for 25 of 27 domains in the State's executive branch.
- Reviewed password and other security related properties for selected Active Directory accounts.
- Reviewed controls over privileged accounts and privileged access.
- Reviewed DTMB's processes for patching domain controllers.
- Verified the installation of antivirus software and reviewed the software definition dates for 25 judgmentally selected domain controllers.

OBJECTIVE #3

To evaluate the effectiveness of the State's controls to add, modify, and delete Active Directory accounts.

To accomplish this objective, we:

- Tested 154 judgmentally selected Active Directory user accounts to determine if the account creation was approved by an authorized requestor and that only the

access requested was granted. We grouped 25 domains by 7 administrative groups. For each administrative group, we randomly selected and tested accounts managed by the particular group.

- Tested 34 judgmentally selected employee transfers from HRMN to determine if the employee's account was modified in an accurate and timely manner.

- Tested 80 judgmentally selected employee departures from HRMN to determine if the employee's account was disabled or deleted in a timely manner.

- Evaluated DTMB's processes for periodically recertifying Active Directory user accounts.

Because the items tested were judgmentally selected, we could not project our results to the respective populations.

CONCLUSIONS

We base our conclusions on our audit efforts and any resulting material conditions or reportable conditions.

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

AGENCY RESPONSES

Our audit report contains 16 findings and 17 corresponding recommendations. DTMB and the separate State agency's preliminary response indicated that they agree with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion at the end of our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

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.
baseline configuration	A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
Center for Internet Security (CIS)	A not-for-profit organization that establishes and promotes the use of consensus-based best practice standards to raise the level of security and privacy in IT systems.
configuration	The way a system is set up. Configuration can refer to either hardware or software or the combination of both.
configuration management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.
Configuration Management Database (CMDB)	A repository that acts as a data warehouse for IT environments. It holds data relating to a collection of IT assets.
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 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.
directory service	Repository of network operating system information to manage users and other resources in a network.
domain	An administrative partition within a forest to manage objects, such as users, groups, and computers. The domain supports a number of core functions related to administration, such as authentication and configuration management.

domain controller	A server with Active Directory installed.
DTMB	Department of Technology, Management, and Budget.
EASA	Enterprise Architecture Solution Assessment.
effectiveness	Success in achieving mission and goals.
efficiency	Achieving the most outputs and the most outcomes practical with the minimum amount of resources.
forest	The outermost design element or boundary in an Active Directory implementation.
group	An object in Active Directory that can have members. Members can be users, contacts, computers, or other groups.
group policy	Policies linked to Active Directory domains, organizational units, or groups, which are applied to the child objects within. Group policies are defined in group policy objects.
group policy object	A collection of settings that define what a system will look like and how it will behave for a defined group of users.
Human Resources Management Network (HRMN)	The State's integrated human resources system that processes personnel, payroll, and employee benefits data.
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.

MiID	DTMB's Active Directory user provisioning tool.
National Institute of Standards and Technology (NIST)	An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.
operating system	The essential program in a computer that manages all the other programs and maintains disk files, runs applications, and handles devices such as the mouse and printer.
operating system administrator	The person responsible for administering use of a multi-user computer system, communications system, or both.
organizational unit (OU)	An Active Directory component that acts as a container to uniformly manage administrative groupings of users, groups, and computers. Security settings are consistently applied to all the computers in an organizational unit by linking the appropriate group policy.
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 access	Extensive system access capabilities granted to persons responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.
privileged account	An account that has access to all commands and files on an operating system or database management system.
reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit

	objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.
RFC	request for change.
risk assessment	The process of identifying risks to entity operations (including mission, functions, image, or reputation), entity assets, or persons by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Risk assessment is a part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
segregation of duties	Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.
server	A computer with a server operating system that can share resources in a network.
threat	An activity, intentional or unintentional, with the potential for causing harm to an automated information system or activity.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

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