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