OAG
Office of the Auditor General

Report Summary

Performance Audit

Statewide Microsoft SQL Database Controls

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0571-19

Released:
June 2020

DTMB maintains approximately 4,200 Microsoft SQL databases that State agencies use for transaction processing and reporting by the State's various IT systems. DTMB Agency Services includes database administrator (DBA) teams that manage the SQL databases. Database security and access controls are the responsibility of the DBA teams in conjunction with the data owners at the various State agencies.

Audit Objective	Conclusion
Objective #1: To assess the effectiveness of DTMB's governance structure over the Microsoft SQL database environment.	Moderately effective

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

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

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

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
Forty-six percent of databases tested did not have encryption-in-transit turned on to minimize the risk of sensitive or confidential data being inadvertently disclosed or accessed during transmission (Finding #4).	X		Agrees
None of the DBA teams selected were aware of new vulnerability management processes that DTMB had implemented. Also, over half of the DBAs and their supervisors did not have access to the new scanning tool. In addition, 50% of tested databases had vulnerabilities that were not remediated in a timely manner (Finding #5).	X		Agrees
Ninety-two percent of the DBA teams sampled could not provide evidence of periodic user database account recertification to ensure that access was still necessary or appropriate. Thirty-three percent of the user accounts reviewed either no longer required access or had excessive privileges. Also, 60% of tested DBAs were using a privileged account that did not have appropriate password complexities (Finding #6).	X		Agrees
Eighty-three percent of the DBA teams selected did not fully monitor high-risk privileged and non-privileged user activity on the database. Also, 50% of the DBA teams selected did not enable audit logging. In addition, 83% of the DBA teams selected did not define high-risk events that, when triggered, would generate an alert (Finding #7).	X		Agrees

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General