Office of the Auditor General
Performance Audit Report

MiWaters
Department of Environmental Quality and
Department of Technology, Management, and Budget

March 2018

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

761-0592-17

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

MiWaters

Department of Environmental Quality (DEQ) and Department of Technology, Management, and Budget (DTMB)

Report Number:
761-0592-17

Released:
March 2018

MiWaters is a Web-based permitting and compliance system implemented in 2015 that replaced over 25 applications and databases used by the DEQ Water Resources Division. MiWaters streamlined DEQ's electronic permitting process, allowing DEQ to fulfill federal electronic reporting requirements and providing an online component for access to public information. MiWaters processes approximately 9,000 permits yearly. MiWaters was developed by a third-party vendor that continues to provide post-implementation enhancements. DTMB provides IT services to DEQ for MiWaters, such as database and operating system support.

Audit Objective			Conclusion
Objective #1: To assess the effectiveness of DEQ and DTMB's security, access, and contingency planning controls over MiWaters.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
MiWaters security could be enhanced with more comprehensive vulnerability scans. Also, MiWaters contingency planning needs improvement (Finding #1).		X	Agrees
MiWaters needs more fully established and implemented access controls. Forty-eight (80%) of 60 judgmentally selected accounts had access rights in excess of those necessary for users to perform their jobs (Finding #2).		X	Agrees

Audit Objective			Conclusion
Objective #2: To assess the effectiveness of DEQ and DTMB's efforts to ensure vendor compliance with the MiWaters contract.			Effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
None reported.	Not applicable.		

Audit Objective			Conclusion
Objective #3: To assess the effectiveness of DEQ and DTMB's efforts to ensure the integrity of MiWaters data.			Effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
None reported.	Not applicable.		

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

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

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

OAG
Office of the Auditor General
Doug A. Ringler, CPA, CIA
Auditor General
201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • audgen.michigan.gov

March 16, 2018

Ms. C. Heidi Grether, Director
Department of Environmental Quality
Constitution Hall
Lansing, Michigan
and
Mr. David L. DeVries
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Ms. Grether and Mr. DeVries:

This is our performance audit report on MiWaters, Department of Environmental Quality and Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agencies 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

MIWATERS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

SECURITY, ACCESS, AND CONTINGENCY PLANNING CONTROLS

BACKGROUND

Security and access controls prevent the compromise of system resources against inappropriate or undesired user access and should be applied to both an application system and a database. Contingency planning helps minimize the impact on systems, business operations, and organizations caused by sudden unplanned events.

The Federal Information System Controls Audit Manual* (FISCAM) is a methodology developed by the U.S. Government Accountability Office (GAO) for performing information system control audits of governmental entities in accordance with professional standards.

There are several vendors in the industry that offer a variety of vulnerability scanning products that enable organizations to detect and classify security weaknesses in networks and systems at the operating system, database, and application level.

AUDIT OBJECTIVE

To assess the effectiveness* of the Department of Environmental Quality (DEQ) and Department of Technology, Management, and Budget's (DTMB's) security, access, and contingency planning controls over MiWaters.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- DTMB performed some vulnerability scans of the MiWaters operating system.
- In fiscal year 2017, DEQ filled its information security officer position.
- Reportable conditions* related to improved security management program and MiWaters access controls (Findings #1 and #2).

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

FINDING #1

MiWaters' security management program could be enhanced.

DEQ, in conjunction with DTMB, should improve its security management program to mitigate the risk of a system disruption and ensure the integrity and confidentiality of MiWaters data.

The departments should:

a. Enhance their vulnerability management process. Specifically:

(1) Vulnerability identification would be improved if DTMB utilized all available vulnerability scanning tools. These tools could be used to detect various types of security weaknesses in the MiWaters operating system, database, and application, depending on the tool used.

DEQ and DTMB used only 1 of 3 available vulnerability scanning tools.

DTMB used one of the scanning tools to perform a monthly Payment Card Industry security vulnerability scan. However, DTMB did not use its scanning tool that can detect security weaknesses unique to the application on the Internet, even though portions of MiWaters are accessible to anyone on the Internet.

Utilizing the other two scanning tools would provide a more holistic view of the threat landscape and increase DTMB's likelihood of detecting and remediating vulnerabilities.

Although the State of Michigan (SOM) Technical Standard 1340.00.150.01 requires that a vulnerability scan be performed a minimum of every 30 days, the Standard does not provide guidance as to which types of scans are required.

(2) DTMB does not have a formal communication process to report to DEQ the vulnerabilities identified by the scans as well as planned mitigation and remediation actions. As the business owner, DEQ should be aware of potential risks and mitigation actions to compare against its operational requirements and determine the actions that best balance functionality and security.

b. Improve their data classification process.

MiWaters contains confidential and sensitive data that should be stored in a secure manner. Without a thorough periodic review of MiWaters data, DEQ cannot adequately communicate to DTMB the appropriate level of controls needed to ensure the confidentiality, integrity, and availability of the data. Specifically:

(1) DEQ had not formalized and implemented a data classification policy and procedure to ensure that the classification of all data elements has been assessed,

roles and responsibilities of the individuals involved in the process have been defined, and evidence supporting the data classification results has been documented and maintained.

DEQ provided us with the results of a data classification review that it conducted in December 2015. However, DEQ was unable to provide adequate evidence to support management's data classification conclusions.

(2) DEQ did not periodically review and reevaluate the classification of MiWaters data to identify new data that needs to be classified and to ensure that the existing classification remains appropriate.

SOM Technical Standard 1340.00.150.02 requires each agency to identify its data that is collected, processed, stored and/or transmitted and establish a process to continually monitor and periodically review and reevaluate the classification of the data.

c. Perform adequate contingency planning.

Without a contingency plan, DEQ and DTMB may be unable to timely restore MiWaters in the event of a disruption.

SOM Technical Standard 1340.00.070.02 requires each agency to create disaster recovery and business continuity plans that incorporate all systems and address all aspects of business resumption. We noted:

(1) DEQ and DTMB did not establish a disaster recovery plan to define roles and responsibilities and the process for restoring MiWaters in the event of a disruption in service.

(2) DEQ's business continuity plan does not provide guidance for the continuation of normal business functions in its 9 field and district offices in the event MiWaters is not in operation. The lack of a business continuity plan could affect over 300 DEQ employees and contractors who perform activities such as permit application processing, service request processing, electronic submittal of compliance schedules, compliance inspection, violation determination, compliance and enforcement action initiation and coordination, and complaint submittal and follow-up.

RECOMMENDATION

We recommend that DEQ, in conjunction with DTMB, improve its security management program to mitigate the risk of a system disruption and ensure the integrity and confidentiality of MiWaters data.

AGENCY PRELIMINARY RESPONSE

DEQ provided us with the following response:

DEQ agrees with the recommendation. DEQ, in conjunction with DTMB, will continue to implement improvements to its security management. Some enhancements were implemented during the audit process, such as the inclusion of IBM's App Scan tool to supplement DTMB's current scanning process. Efforts to strengthen DEQ's business continuity and disaster recovery plans are in process and scheduled to be completed no later than December 31, 2018.

FINDING #2

DEQ did not implement effective access controls to ensure the security of MiWaters data.

Improved access controls are needed.

SOM Technical Standard 1340.00.020.01 requires the establishment of a process to control and document the assignment of access rights based on current job responsibilities and the principle of least privilege* and requires agencies to review accounts for compliance every 120 days. Also, SOM Technical Standard 1340.00.040.01 requires the use of audit logs to record user activities and security events to maintain a proper audit trail and assist in monitoring access.

DEQ did not:

No process existed for granting and removing access or periodic review of access rights.

a. Establish a formal process to grant and remove access to MiWaters, including the use of a standard authorization form to document business owner approval of the access rights granted to users.

   After bringing this matter to management's attention, DEQ began developing a documented process and a standardized authorization form.

b. Periodically review user access rights.

   DEQ had not performed a comprehensive review of user access rights subsequent to MiWaters' implementation in 2015. Periodic reviews help ensure that privileges granted to each user remain appropriate for the user's job responsibilities.

c. Grant access to MiWaters based on the principle of least privilege.

   We judgmentally selected and tested 60 user accounts to test the appropriateness of access rights granted to the account. The following chart summarizes our user access exceptions:

Organization	Accounts Tested	Accounts With Excessive Permissions	Development Accounts With Access to Production	Generic Accounts
DEQ	25	14 (56%)	0 (0%)	0 (0%)
DTMB	4	3 (75%)	0 (0%)	1 (25%)
Third-party vendor	31	31 (100%)	31 (100%)	21 (68%)
Total	60	48 (80%)	31 (52%)	22 (37%)

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

We noted:

(1) Forty-eight (80%) of 60 accounts did not require some or all of the assigned access rights based on the users' job responsibilities. DEQ indicated that 10 (21%) of the 48 accounts were used for pre-implementation testing purposes and should be inactivated. DEQ should limit access rights to only those necessary for users to perform their day-to-day tasks to reduce the potential for inappropriate use of MiWaters.

(2) Thirty-one (52%) of 60 accounts belonged to third-party vendor development staff. Seven (23%) of the 31 developer accounts had high-risk user access rights. Developers should not be granted access to production data to reduce the risk of unauthorized access and modification of MiWaters data.

(3) Twenty-two (37%) of 60 accounts were generic accounts not associated with a specific user. DEQ indicated that 21 (95%) of the 22 accounts were used for pre-implementation testing purposes and should be inactivated. Eliminating generic accounts from MiWaters can increase accountability for actions performed in MiWaters.

d. Routinely monitor audit logs for inappropriate activity, in conjunction with DTMB.

Monitoring of the logs can assist in identifying security incidents, policy violations, fraudulent activity, and operational problems along with providing information useful for resolving such problems.

DTMB informed us that the MiWaters database has no audit logs that would identify privileged activity beyond tracking general login information.

e. Ensure that the read-only security group could not make changes to MiWaters data.

A read-only security group should allow users to view information only. We tested the capabilities of the read-only security group and determined that the group inappropriately had the ability to change MiWaters data, such as editing permit violations.

RECOMMENDATION We recommend that DEQ implement effective access controls to ensure the security of MiWaters data.

AGENCY PRELIMINARY RESPONSE

DEQ provided us with the following response:

DEQ agrees with the recommendation. DEQ will continue to evaluate access controls and implement process improvements while documenting known risks and mitigating efforts accordingly. Several reviews and approval processes have been revised to provide greater control over MiWaters' data security. Full documentation regarding access controls, process reviews, and known risks will be implemented by December 31, 2018.

VENDOR COMPLIANCE WITH THE MIWATERS CONTRACT

BACKGROUND

In May 2013, the State entered into a five-year contract with a third-party vendor to develop and provide post-implementation enhancements for MiWaters. MiWaters was implemented in August 2015.

AUDIT OBJECTIVE

To assess the effectiveness of DEQ and DTMB's efforts to ensure vendor compliance with the MiWaters contract.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- No significant weaknesses were identified related to contract deliverables.
- DEQ and DTMB held regular meetings with the vendor to discuss upcoming releases, enhancements, maintenance, and other concerns of the agencies and vendor.

INTEGRITY OF MIWATERS DATA

BACKGROUND

MiWaters is a Web-based permitting and compliance system that is used by DEQ, permittees and permit applicants, and the general public. MiWaters allows users to electronically submit applications and requires documentation such as discharge monitoring reports, annual reports, and corrective action plans. In addition, MiWaters facilitates the electronic transfer of data required by the U.S. Environmental Protection Agency (EPA) for all National Pollutant Discharge Elimination System (NPDES) permittees.

AUDIT OBJECTIVE

To assess the effectiveness of DEQ and DTMB's efforts to ensure the integrity of MiWaters data.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- No significant data integrity weaknesses were identified in MiWaters.

SYSTEM DESCRIPTION

MiWaters is a Web-based permitting and compliance system that replaced more than 25 applications and databases used by the DEQ Water Resources Division. MiWaters established a streamlined electronic permitting process, allowing Michigan to fulfill federal electronic reporting requirements and providing online access to public information. The focus of MiWaters is permitting and compliance for NPDES, storm water, groundwater discharge, aquatic nuisance control, Part 41 construction, and land and water interface permits. MiWaters also provides electronic reporting of untreated or partially treated sanitary wastewater.

As of April 2017, approximately 355 internal users and 14,000 external public users use MiWaters. MiWaters processes approximately 9,000 permits yearly.

MiWaters was developed and is supported by a third-party vendor. DTMB provides IT support services to DEQ for MiWaters, including operating system configuration, database administration, back-up and recovery, change management, operational support for the test and production environments, and access security.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the information processing and other records of MiWaters. 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 October 1, 2014 through May 31, 2017.

METHODOLOGY

We conducted a preliminary survey of MiWaters. During our preliminary survey, we:

- Interviewed DEQ Water Resources Division and DTMB management and staff to gain an understanding of MiWaters.
- Reviewed the contract for MiWaters development.
- Reviewed DEQ and DTMB policies and procedures related to MiWaters and MiWaters security.
- Obtained an understanding of DEQ's and DTMB's processes for:
    - The various MiWaters modules, including permitting, service requests/applications, inspections and evaluations, submittals, compliance and enforcement, financials and invoicing, and incidents/complaints/spills.
    - Granting, monitoring, and removing user access to the MiWaters application and database.

OBJECTIVE #1

To assess the effectiveness of DEQ and DTMB's security, access, and contingency planning controls over MiWaters.

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

To accomplish this objective, we:

- Obtained a list of 355 active internal MiWaters user accounts as of April 2017. We judgmentally selected and reviewed 60 accounts to assess whether DEQ:
    - Followed the principle of least privilege when assigning roles and privileges to users.
    - Timely deactivated user accounts of terminated employees and third-party users.
    - Timely deactivated accounts of users who no longer had a valid business purpose to access MiWaters.
- Interviewed DEQ personnel to determine whether a formal access authorization process was implemented and periodic review of user access rights was performed.
- Reviewed system documentation to determine if DEQ and DTMB completed and documented MiWaters risk assessment, security plan, and contingency plan.
- Interviewed DTMB personnel to determine if monthly vulnerability scans are performed on MiWaters servers.
- Reviewed application and database security settings and assessed whether high-risk actions are monitored.
- Assessed the roles and responsibilities of DEQ's security officer regarding MiWaters.

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

OBJECTIVE #2

To assess the effectiveness of DEQ and DTMB's efforts to ensure vendor compliance with the MiWaters contract.

To accomplish this objective, we:

- Judgmentally selected 23 out of approximately 116 contract deliverables to assess whether the deliverables were completed as outlined in the contract.
- Observed a meeting between DEQ and DTMB management and the third-party vendor regarding system enhancements and maintenance.

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

OBJECTIVE #3

To assess the effectiveness of DEQ and DTMB's efforts to ensure the integrity of MiWaters data.

To accomplish this objective, we:

- Tested MiWaters for missing and inaccurate data.
- Reviewed and tested the interface of MiWaters data from May 2 through May 9, 2017 between DEQ and the EPA.

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 2 findings and 2 corresponding recommendations. DEQ's preliminary response indicates that it agrees with both 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 fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it 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.

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

GLOSSARY OF ABBREVIATIONS AND TERMS

DEQ	Department of Environmental Quality.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
EPA	U.S. Environmental Protection Agency.
Federal Information System Controls Audit Manual (FISCAM)	A methodology published by the U.S. Government Accountability Office (GAO) for performing information system control audits of federal and other governmental entities in accordance with *Government Auditing Standards*.
IT	information technology.
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.
NPDES	National Pollutant Discharge Elimination System.
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.
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.
SOM	State of Michigan.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

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