Office of the Auditor General
Performance Audit Report

Investment-Related Systems
Bureau of Investments
Department of Treasury and
Department of Technology, Management, and Budget

May 2016

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

271-0585-15

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
Investment-Related Systems
Bureau of Investments
Department of Treasury and Department of Technology, Management, and Budget

Report Number:
271-0585-15

Released:
May 2016

The Bureau of Investments (BOI) provides investment management services, professional expertise, and advice to the State Treasurer as fiduciary of the State of Michigan retirement systems and Michigan boards and agencies. BOI uses a portfolio management and investment accounting system (Q2) to manage and track $74.6 billion of the State's publicly and privately held investments. BOI uses Bloomberg Asset Investment Manager (AIM) to manage and trade the State's public investments. The Department of Technology, Management, and Budget (DTMB) is responsible for maintaining, supporting, and securing the servers upon which Q2 is stored and processed.

Audit Objective	Conclusion
Objective #1: To assess the effectiveness of BOI and DTMB's security and access controls over Q2.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
BOI, in conjunction with DTMB, did not fully establish and implement security and access controls over the Q2 application to ensure the authorization and authentication of users and the protection of Q2 data. BOI did not document 12 (55%) of 22 users' authorization, did not monitor audit logs for inappropriate access, and did not recertify access authorization for 10 (45%) of 22 users every 120 days according to DTMB standards (Finding #1).		X	Agrees
DTMB, in conjunction with BOI, did not fully establish and implement security and access controls over the Q2 database, which may increase the risk of data loss and unauthorized modification. For example, 16 (41%) of 39 security settings were not in compliance with best practices; three accounts did not require a password to access the database, two of which also did not require a user ID to log in; and the third party vendor used group accounts, which limited the ability to trace account activity to a unique individual (Finding #2).		X	Agrees

Audit Objective			Conclusion
Objective #2: To assess the effectiveness of BOI's access controls over Bloomberg AIM.			Effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
BOI did not fully implement access controls to ensure the authorization of Bloomberg AIM users by properly documenting authorized access, monitoring audit logs for inappropriate activity, or reviewing access rights every 120 days according to DTMB standards (Finding #3).		X	Agrees

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: www.audgen.michigan.gov

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 • www.audgen.michigan.gov

May 13, 2016

Mr. Nick A. Khouri
State Treasurer
Richard H. Austin Building
Lansing, Michigan
and
Mr. David B. Behen
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Mr. Khouri and Mr. Behen:

I am pleased to provide this performance audit report on Investment-Related Systems, Bureau of Investments, Department of Treasury and Department of Technology, Management, and Budget.

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

TABLE OF CONTENTS

INVESTMENT-RELATED SYSTEMS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

SECURITY AND ACCESS CONTROLS OVER Q2

BACKGROUND

Q2 is a vendor-managed investment accounting system used by the Bureau of Investments (BOI) to manage and track the State's investments.

Security* and access controls* limit or detect inappropriate access, which is important to ensure the availability, confidentiality, and integrity of data.

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.

The Center for Internet Security* (CIS) establishes and promotes best practice standards to raise the level of security and privacy in information technology* (IT) systems.

AUDIT OBJECTIVE

To assess the effectiveness* of BOI and the Department of Technology, Management, and Budget's (DTMB's) security and access controls over Q2.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- No identified instances of inappropriate user access to Q2.
- The Q2 application does not contain confidential data.
- Multi-factor security access controls were in place.
- Establishment and implementation of some security configurations* and access controls in accordance with State policy and best practices, such as invalid password and terminal lockout controls.
- Reportable conditions* related to improved Q2 application security and access controls (Finding #1) and more comprehensive database* security configurations and user access controls (Finding #2).

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

FINDING #1

Improvements are needed to Q2 application security and access controls.

BOI, in conjunction with DTMB, did not fully establish and implement security and access controls over the Q2 application to ensure the authorization and authentication of users and the protection of Q2 data.

FISCAM states that user access should be limited to individuals with a valid business purpose, access authorization forms should be maintained, and system owners and security managers should periodically monitor user access. FISCAM also recommends that program changes be restricted and monitored.

BOI, in conjunction with DTMB, did not:

a. Document the authorization of Q2 user access rights.

   BOI informed us that it reviews user access rights annually. However, 12 (55%) of 22 Q2 users did not have documented authorization of their access rights to help ensure that only appropriate individuals have access to Q2 and that the rights assigned to them are appropriate. BOI informed us that it will implement a procedure to print, sign, and date applicable documentation as evidence of its review.

b. Routinely monitor the appropriateness of user activity.

   BOI informed us that audit logs are available in Q2 and are used for troubleshooting purposes. In addition, BOI performs various account reconciliations with third party sources to ensure that account data is accurate. However, without routine monitoring of audit logs for atypical user activity, such as several failed log-in attempts on multiple accounts, inappropriate user activity may go undetected. In addition, user awareness that routine monitoring occurs can be a deterrent to inappropriate activity.

c. Periodically review user access rights every 120 days to ensure that rights remain appropriate.

   DTMB Technical Standard 1335.00.03 requires that user access be reviewed every 120 days. BOI currently recertifies access annually in accordance with Department of Treasury policy ET-03179; however, DTMB Administrative Guide policy 1305.00 requires that internal agency policies complement and comply with DTMB policy. In addition, 10 (45%) of 22 active users were not documented in writing on BOI's annual recertification.

d. Periodically review and update the Q2 security plan.

   The Q2 security plan was not periodically reviewed and updated every three years in accordance with Department of Treasury policy. An updated security plan helps reflect

system and organization changes, problems identified during plan implementation, and security control assessments.

RECOMMENDATION

We recommend that BOI, in conjunction with DTMB, fully establish and implement security and access controls to properly protect the Q2 application and data.

AGENCY PRELIMINARY RESPONSE

BOI and DTMB provided us with the following response:

BOI believes there is low risk of unauthorized or inappropriate access to the Q2 application, which does not maintain any personal, tax, or exempt information. In addition, multi-factor security access controls are in place.

a. *BOI partially agrees with this recommendation. All user access rights are reviewed annually. Going forward, as evidence of the review, all applicable documentation will be printed, signed, and dated.*

b. *BOI partially agrees with this recommendation. All logs are available in Q2 and are used for troubleshooting. Inappropriate use is prohibited by user rights recorded in the application user rights tables and application design. The issue is mitigated since other internal controls are in place to detect inappropriate activity such as matching with third party data.*

c. *BOI agrees with this recommendation. It is noted that BOI complies with an annual review process under Treasury Policy ET-03179 (page 5, item #7), whereby BOI management in the Trust Accounting Division performs an annual review of user access rights for the Q2 application. Historically, BOI does not have employee turnover that would warrant a 120-day recertification review. All users were included in the annual certification. Going forward, BOI will perform a 120-day recertification review, with all applicable documentation printed, signed, and dated as evidence of the review.*

d. *BOI and DTMB agree with this recommendation. The departments are in the process of upgrading the Q2 application with a vendor-hosted QED Q2 system and PaaS (Platform as a Service/Cloud) implementation. The upgrade project also includes completing a security plan (i.e., the DTMB-170), which will be reviewed periodically per policy.*

In summation, BOI and DTMB are working with QED to upgrade the Q2 application to fully establish and implement security and access controls. It is anticipated that the upgrade will be completed by May 2016, barring any unforeseen issues.

FINDING #2

More comprehensive security configurations and user access controls are vital to protecting the Q2 database.

DTMB, in conjunction with BOI, did not fully establish and implement security and access controls over the Q2 database, which may increase the risk of data loss and unauthorized modification.

Finding #1 addressed access to the Q2 application. This finding involves the database that manages and protects Q2 data.

DTMB Technical Standard 1340.00.15 requires database administrators to implement security controls to prevent unauthorized access. Implementation of these controls will provide best practices toward data confidentiality, integrity, and risk management.

DTMB, in conjunction with BOI, did not:

a. Ensure the effective configuration of Q2 database security settings, such as profile settings and configuration parameters.

16 (41%) of 39 security settings were not in compliance with best practices.

We reviewed 39 security settings and noted that 16 (41%) were not in compliance with best practices. Proper configuration of the database security settings reduces the risk of loss or unauthorized access to data. Noncompliant settings included:

- Improper system file permissions.
- Outdated security patches.
- Unenforced password policy parameters.

Because of the confidential nature of security settings, detailed results were summarized and provided to DTMB and BOI.

b. Sufficiently restrict access to the Q2 database.

Three accounts did not require a password to access the database, two of which also did not require a user ID to log in. In addition, the third party vendor used group accounts, which limited the ability to trace account activity to a unique individual to ensure that only authorized individuals had access.

c. Document and maintain the authorization and approval of user access to the Q2 database.

DTMB and BOI did not document authorization of vendor access to the database, including the rights granted to each vendor account. In addition, DTMB and BOI were unable to periodically recertify user access in accordance with DTMB policy because of the lack of access

documentation. Documentation helps ensure that only appropriate individuals have access to the database and that privileges assigned to them are appropriate.

d. Use database audit logs to monitor the activity of database administrators and other privileged accounts*.

   Audit logs were not configured to capture account activity, which can help identify unusual or unauthorized actions. Recording and monitoring selected high-risk actions by privileged accounts would enhance database security.

Security and access controls over the Q2 database were not fully established and implemented because DTMB and BOI management did not establish procedures to ensure that the third party vendor complied with industry best practices and State policies and procedures.

RECOMMENDATION

We recommend that DTMB, in conjunction with BOI, fully establish and implement security and access controls over the Q2 database.

AGENCY PRELIMINARY RESPONSE

BOI and DTMB provided us with the following response:

DTMB and BOI agree with the recommendation. The Q2 application is in the process of being upgraded to a newer system that will resolve many of the noted issues. BOI anticipates that the upgrade will be completed by May 2016, barring any unforeseen issues.

As part of the Statement of Work (SOW) for the upgrade project, the Q2 software application will be moved from the State of Michigan servers to QED vendor-hosted servers for the remaining two option years of the contract. In addition, the SOW project plan establishes tasks for the upgrade of the Q2 software to the current version.

a. The security settings for the Q2 database shall be in compliance with best practices commensurate with the upgrade of the Q2 software defined in the SOW and in accordance with the architecture of the QED platform.

b. The upgrade to the current version of the Q2 software provided as a service shall include a managed MySQL version in which blank passwords and anonymous accounts are programmatically prohibited as an installation, configuration, and provisioning best practice. Further, the Q2 software shall be configured in accordance with BOI and DTMB requirements to include named MySQL maintenance accounts for QED staff.

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

c. *Consistent with State of Michigan policies as applicable to DTMB and BOI, the service level agreement will define the requirements for the Q2 software provided as a service, including standard operating procedures for the definition and maintenance of authorized and approved QED and client staff user accounts.*

d. *The upgrade to the current version of the Q2 software provided as a service shall include a managed MySQL version in which Enterprise Audit Logging features are programmatically enabled during installation, configuration, and provisioning.*

In summation, BOI and DTMB will work with QED, the vendor of the Q2 database application, to fully establish and implement security and access controls within the Q2 system upgrade.

ACCESS CONTROLS OVER BLOOMBERG AIM

BACKGROUND

Bloomberg Asset and Investment Manager (AIM) is a third party solution used by BOI to manage and trade public investments.

AUDIT OBJECTIVE

To assess the effectiveness of BOI's access controls over Bloomberg AIM.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- Only appropriate personnel had access to Bloomberg AIM for the initiation, approval, and execution of trades.
- Establishment and implementation of some user access controls in accordance with State policy and best practices:
    - Bloomberg AIM has a two-factor authentication process.
    - BOI developed a separation of duties* matrix to ensure that users are not granted conflicting access rights in Bloomberg AIM, such as the ability to both initiate and approve a trade.
- Reportable condition related to improved access controls (Finding #3).

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

FINDING #3

BOI did not fully implement access controls to ensure the authorization of Bloomberg AIM users.

Improvements are needed to Bloomberg AIM access controls.

FISCAM states that access controls should be implemented at the application level to provide reasonable assurance that only authorized personnel have access.

BOI did not:

a. Document authorization of user access to Bloomberg AIM.

   BOI informed us that it reviews user access rights annually and that a contract is required for each Bloomberg AIM user license. However, BOI did not have a standardized form to document business owner approval of specific access rights being granted to new users. Documenting the authorization of access helps to ensure that only appropriate individuals have access to Bloomberg AIM and that the access rights assigned are appropriate. BOI informed us that it will implement an authorization form by the end of March 2016 to document authorization for all users.

b. Document its reviews of user activity and account management logs.

   BOI informed us that it performs a daily review of user activity and account management logs. However, BOI did not document its review of the logs. Routine monitoring, as evidenced by formal documentation, will help ensure the detection of inappropriate user activity. BOI informed us that it will implement a procedure for documenting its review of audit logs with an electronic signature and date.

c. Periodically review user access rights every 120 days to ensure that rights remain appropriate.

   DTMB Technical Standard 1335.00.03 requires that user access be reviewed every 120 days. BOI currently recertifies access annually in accordance with Department of Treasury policy ET-03179; however, DTMB Administrative Guide policy 1305.00 requires that internal agency policies complement and comply with DTMB policy.

RECOMMENDATION

We recommend that BOI fully implement access controls to ensure the authorization of Bloomberg AIM users.

AGENCY PRELIMINARY RESPONSE

BOI provided us with the following response:

BOI agrees with the recommendation and believes the risk of unauthorized or inappropriate access to the Bloomberg AIM system is low. Also, multi-factor security access controls are in place. In addition, BOI has a separation of duties matrix to ensure that users are not granted conflicting access rights in Bloomberg AIM.

a. *To address this issue, BOI has developed a Bloomberg New User/Change Request Form, which will document authorization for all future users of the Bloomberg AIM system.*

b. *The Bloomberg AIM audit logs are maintained and can be accessed at any time but cannot be modified or deleted. The ability to download audit logs eliminates the risk of modification or deletion. Best practices recommend that audit logs be stored outside of the system. Going forward, the audit logs will be electronically signed and dated for security purposes, which will further mitigate any potential concerns.*

c. *While BOI complies with the annual review requirements of Treasury Policy ET-03179 whereby the BOI Bloomberg Transaction Manager and BOI administration perform an annual review of user access rights for the Bloomberg AIM system, BOI will comply with DTMB standard 1335.00.03 and perform a 120-day review of user access rights. As evidence of the review, all applicable documentation will be printed, signed, and dated.*

In summation, BOI will fully implement the aforementioned access controls for the Bloomberg AIM system.

SYSTEM DESCRIPTION

BOI provides investment management services, professional expertise, and advice to the State Treasurer as fiduciary of the State of Michigan retirement systems and Michigan boards and agencies. BOI uses the following systems to manage and track the State's publicly and privately held investments:

- Q2 is a vendor-managed system used to manage and track the State's $74.6 billion of publicly and privately held investments as of September 30, 2015. Q2 interfaces with the State's financial management system, the Michigan Administrative Information Network (MAIN), in order to record investment activity on the State's financial statements.

- Bloomberg AIM is an integrated suite of solutions designed for buy-side institutions, hedge funds, and proprietary trading desks. BOI uses Bloomberg AIM for managing and trading the State's public investments.

DTMB Technical Services is responsible for maintaining, supporting, and securing the servers upon which Q2 is stored and processed.

DTMB Agency Services is responsible for delivering and coordinating IT services.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the program and other records of BOI's investment-related systems (Q2 and Bloomberg AIM). 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 the period October 1, 2013 through September 30, 2015.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of investment-related systems to establish our audit objectives and methodology. This included gaining an understanding of DTMB policies and procedures for State of Michigan IT systems. During our preliminary survey, we:

- Interviewed BOI management and staff to obtain an understanding and a walk-through of Q2 and Bloomberg AIM.
- Reviewed the Department of Treasury and DTMB security and access control policies and procedures applicable to Q2 and Bloomberg AIM.
- Reviewed system documentation.
- Reviewed the vendor's SOC 1 report* for Q2.
- Reviewed industry best practices for database security developed by CIS.
- Obtained an understanding of BOI's processes for:
    - Granting user access to Q2 and Bloomberg AIM.
    - Determining what roles/privileges are assigned to users.
    - Approving and implementing updates and security patches to Q2.

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

OBJECTIVE #1

To assess the effectiveness of BOI and DTMB's security and access controls over Q2.

To accomplish our first objective, we:

- Assessed the business continuity plan established by BOI for Q2.
- Obtained the security plan for Q2 to determine if BOI and DTMB:
    - Followed industry best practices and Department of Treasury policy.
    - Periodically reviewed the security plan and risk assessment*.
- Reviewed industry best practices and Department of Treasury and DTMB policies related to configuration management* and change controls* to determine if BOI and DTMB:
    - Documented, tested, and monitored changes made.
    - Established procedures for emergency changes.
- Obtained knowledge of vendor change management techniques.
- Obtained a list of active Q2 users and user access forms to determine whether BOI:
    - Periodically recertified active user accounts.
    - Timely deactivated user accounts of users no longer employed.
    - Actively monitored and documented user activity logs.
    - Established access authentication parameters according to DTMB policy.
- Reviewed the Q2 separation of duties matrix to identify conflicting transactions and activities.

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

OBJECTIVE #2

To assess the effectiveness of BOI's access controls over Bloomberg AIM.

To accomplish our second objective, we:

- Obtained a list of active Bloomberg AIM users and assessed whether:
    - Access authentication parameters complied with DTMB policy.
    - BOI periodically recertified active user accounts.
- Reviewed user access forms and tested for compliance with DTMB policy.
- Reviewed separation of duties matrices to determine whether any conflicting access rights were granted.

CONCLUSIONS

We base our conclusions on our audit efforts and the resulting material conditions* and 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 3 findings and 3 corresponding recommendations. BOI and DTMB's preliminary response indicates 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.

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

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.
AIM	Asset and Investment Manager.
BOI	Bureau of Investments.
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.
change controls	Controls that ensure that program, system, or infrastructure modifications are properly authorized, tested, documented, and monitored.
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.
database	A collection of information that is organized so that it can be easily accessed, managed, and updated.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
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.*
information technology (IT)	Anything related to computing technology, such as networking, hardware, software, the Internet, or the people who work with these technologies.

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.
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.
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.
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.
separation of duties	Segregation 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.
SOC 1 report	A report prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16 in which an independent auditor reports on management's description of a service

	organization's system and the suitability of the design of controls (a type 1 report). The auditor may be engaged to also test and report on the operating effectiveness of those controls (a type 2 report).
SOW	Statement of Work.

This Page Left Intentionally Blank

This Page Left Intentionally Blank


OAG
Office of the Auditor General
Independent
Objective
Transparent