MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT
ON THE

TERADATA DATA WAREHOUSE

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

September 2010

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

084-0520-04F

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

Audit report information can be accessed at:
http://audgen.michigan.gov

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

September 8, 2010

Mr. Kenneth D. Theis, Director
Department of Technology, Management & Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Theis:

This is our report on our follow-up of the 3 material conditions (Findings 1 through 3) and 3 corresponding recommendations reported in the performance audit of Teradata Data Warehouse, Department of Information Technology (DIT). That audit report was issued and distributed in November 2005; however, additional copies are available on request or at <http://www.audgen.michigan.gov>. In March 2010, subsequent to our original audit, Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management & Budget (DTMB). It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of DIT to DTMB by a Type III transfer and abolished DIT.

Our follow-up disclosed that DTMB had partially complied with the 3 recommendations. However, a material condition still exists for the server security plan recommendation, and reportable conditions exist for the other 2 recommendations.

If you have any questions, please call me or Scott M. Strong, C.P.A., C.I.A., Deputy Auditor General.

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

TERADATA DATA WAREHOUSE
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
FOLLOW-UP REPORT

TERADATA DATA WAREHOUSE
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
FOLLOW-UP REPORT

INTRODUCTION

This report contains the results of our follow-up of the material conditions and corresponding recommendations and the agency's preliminary response as reported in our performance audit of the Teradata Data Warehouse, Department of Information Technology (DIT) (50-520-04), which was issued and distributed in November 2005. That audit report included 3 material conditions (Findings 1 through 3) and 4 other reportable conditions (Findings 4 through 7).

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether the Department of Technology, Management & Budget (DTMB) has taken appropriate corrective measures in response to the 3 material conditions and 3 corresponding recommendations.

BACKGROUND

The State's Teradata data warehouse (Data Warehouse) is a centralized repository of data used to support State agencies' decision-making and business processes. The Data Warehouse contains a large volume of historical data from multiple data sources. Much of the data stored on the Data Warehouse is considered sensitive or confidential. State agencies extract data from source systems, transform and format the data, and load the data into the Data Warehouse. State agencies use analytical tools to combine and query data stored on the Data Warehouse to obtain accurate and timely information to support business decisions and for State and federal reporting.

In March 2010, Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management & Budget (DTMB). It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of DIT to DTMB by a Type III transfer and abolished DIT.

SCOPE

Our fieldwork was performed between February and April 2010. We interviewed employees from DTMB to determine the status of compliance with our audit recommendations. We reviewed the information technology (IT) risk assessment, disaster recovery plan, and policies and procedures for configuring the Data Warehouse servers. We obtained an understanding of the processes used for implementing strong password rules, restricting access, and monitoring activity. We also reviewed select operating system configurations for three Data Warehouse servers.

FOLLOW-UP RESULTS

EFFECTIVENESS OF PROCESSES TO ENSURE THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF DATA

RECOMMENDATION AND RESPONSE AS REPORTED IN NOVEMBER 2005:

1. Server Security Plan

RECOMMENDATION

We recommend that DIT develop a server security plan for the Data Warehouse.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding and will continue to evaluate and implement reasonable cost-effective strategies that mitigate the level of risk to the State's servers. DIT informed us that it has established two positions within the Office of Enterprise Security dedicated to providing security services to existing enterprise platforms. DIT will formalize its strategy for conveying the new Teradata operating system and database management system release information to database administrators.

Lastly, as noted in the audit report, DIT has completed and successfully tested a disaster recovery plan for the Data Warehouse. DIT will work to achieve full compliance by December 31, 2005.

FOLLOW-UP CONCLUSION

We concluded that DTMB had not fully addressed the 4 conditions cited in this finding and, therefore, had only partially complied with the recommendation to develop a server security plan for the Data Warehouse. A material condition still exists. Specifically, our follow-up disclosed:

a. DTMB had not fully completed an assessment of IT risks for the Data Warehouse. DTMB drafted an IT risk assessment, but the assessment was not reviewed and approved by stakeholders. Subsequent to our review, DTMB informed us that it distributed the risk assessment to stakeholders and that DTMB anticipates the assessment will be approved by October 1, 2010.

b. DTMB had not fully completed an updated disaster recovery plan for the Data Warehouse. Subsequent to the original audit, DIT completed a disaster recovery plan in 2005. However, the 2005 disaster recovery plan is no longer relevant to the current environment of the Data Warehouse. DTMB drafted an updated disaster recovery plan, but the plan had not been approved or tested. Subsequent to our review, DTMB informed us that it approved the disaster recovery plan, and a date to test the plan will be scheduled by September 1, 2010.

c. DTMB had not developed procedures for implementing new features of the relational database system. DTMB informed us that new features are reviewed informally. However, DTMB does not have a procedure to evaluate if and how the features should be implemented and to ensure that the database administrators understand, document, and properly implement the new features. Subsequent to our review, DTMB informed us that it developed and published procedures for implementing new features.

d. DTMB had not completely developed standards and guidelines for configuring and securing the operating systems of the Data Warehouse. DTMB informed us that it had developed a process to ensure the operating system is properly configured and secured. However, DTMB has not developed a standard or

guideline to ensure that the process is routinely and consistently applied. Subsequent to our review, DTMB informed us that it developed and published complete standards and guidelines for configuring and securing the operating systems.

RECOMMENDATION AND RESPONSE AS REPORTED IN NOVEMBER 2005:

2. Operating System Security

RECOMMENDATION

We recommend that DIT effectively secure the operating systems of the Data Warehouse servers.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding and will continue to work to effectively secure the Data Warehouse operating system security. DIT informed us that it is currently testing new procedures and will continue to review and implement new security features, such as intrusion detection. DIT informed us that, despite the noted risks, DIT is not aware of any instances in which the confidentiality, integrity, and availability of the Data Warehouse were compromised. DIT will work to achieve full compliance by October 31, 2005.

FOLLOW-UP CONCLUSION

We concluded that DTMB had not fully addressed 3 of the 6 conditions cited in this finding and, therefore, had only partially complied with the recommendation to effectively secure the operating system of the Data Warehouse servers. A reportable condition still exists. We reviewed operating system configurations for 3 of the 12 Data Warehouse servers that were tested in the original audit. Our follow-up disclosed:

a. DTMB assigned unique user codes to privileged users in order to maintain accountability of users when performing job responsibilities.

b. DTMB locked or removed the default system accounts for the 3 servers. However, DTMB did not properly restrict the default system accounts' access

to critical services. Restricting access to critical services further reduces the vulnerability of unauthorized access.

c. DTMB did not completely restrict access to critical operating system configuration files for the 3 servers. The configuration files contain sensitive information that the operating system uses to perform tasks and, typically, ordinary users do not need access to these files.

d. DTMB had not implemented strong password rules for operating system user accounts on 1 of the 3 servers. The implementation of strong password rules reduces the risk of unauthorized access to the operating system.

e. DTMB locked or removed unnecessary operating system services to reduce the risk of unauthorized access to the operating system.

f. DTMB implemented a host-based intrusion detection system to detect unauthorized access to the operating system.

After bringing weaknesses indentified in parts b., c., and d. to DTMB's attention again in 2010, DTMB informed us that it adjusted the configurations to ensure that access to critical services and files were properly restricted and that strong password rules were used on all servers.

RECOMMENDATION AND RESPONSE AS REPORTED IN NOVEMBER 2005:

3. Database Security

RECOMMENDATION

We recommend that DIT establish effective security over the Data Warehouse's database.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding and will continue to work to effectively secure the Data Warehouse database security. DIT informed us that it is currently implementing agency services roles and profiles, creating unique administrator accounts, removing excessive default permissions, and enabling logging and monitoring controls. DIT will work to achieve full compliance by January 31, 2006.

FOLLOW-UP CONCLUSION

We concluded that DTMB had not fully addressed 3 of the 4 conditions cited in this finding and, therefore, had only partially complied with the recommendation to establish effective security over the Data Warehouse's database. A reportable condition still exists. Specifically, our follow-up disclosed:

a. DTMB had not implemented strong password rules for all database user accounts. DTMB issued a recommendation to agency database administrators stating that all database user accounts should use strong password rules. However, our review indicated that strong password rules were not being used for all user accounts. DTMB indicated that it will enforce strong password rules for all users no later than September 1, 2010.

b. DTMB had not established unique database administrator (DBA) user accounts. However, DTMB had implemented a compensating control that ensures accountability for the DBA activity and also provides management with a means to monitor changes to the database. Therefore, DBAs use shared accounts, but the activity on the shared accounts can be connected to a specific individual.

c. DTMB further restricted users' access by assigning users to roles. The role-based methodology for assigning access improves management's ability to assign appropriate access and identify and remove excessive access. Although DTMB has promoted the use of roles in assigning access, DTMB has not completed a review to ensure that all users are assigned to a role and that the role is appropriate. DTMB indicated that it will work with agency representatives to review users' access by September 15, 2010. DTMB also indicated that it will implement a process to review access annually.

d. DTMB did not monitor the activities of privileged users. DTMB developed reports that would allow them to monitor the activities of privileged users. However, DTMB had not established a process, policies, or procedures for reviewing the activity. Subsequent to our review, DTMB informed us that procedures for reviewing privileged activity were created and published.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL