



MICHIGAN

OFFICE OF THE AUDITOR GENERAL



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

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 21, 2012

John E. Nixon, C.P.A., Director
Department of Technology, Management, and Budget
George W. Romney Building
Lansing, Michigan
and
Mr. David B. Behen, Chief Information Officer
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Nixon and Mr. Behen:

This is our report on our follow-up of the 3 material conditions (Findings 1, 6, and 8) and 4 corresponding recommendations reported in the performance audit of Data Center Operations, Department of Information Technology (DIT). That audit report was issued and distributed in July 2007. Additional copies are available on request or at <http://www.audgen.michigan.gov>. In March 2010, subsequent to our performance audit, Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management, and Budget (DTMB). It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of DIT to DTMB and abolished DIT.

Our follow-up disclosed that DTMB had partially complied with the 4 recommendations. A material condition still exists related to the implementation of security over the State's data exchange gateway (DEG) (Finding 8), and reportable conditions exist related to risk assessments for hosting center operations (Finding 1) and the development and testing of disaster recovery plans for the hosting center facilities (Finding 6).

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

Sincerely,



Thomas H. McTavish, C.P.A.
Auditor General

TABLE OF CONTENTS

DATA CENTER OPERATIONS DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET FOLLOW-UP REPORT

	<u>Page</u>
Report Letter	1
Introduction	4
Purpose of Follow-Up	4
Background	4
Scope	5
Follow-Up Results	
Effectiveness in Administering the Hosting Centers	6
1. Risk Assessments	6
Effectiveness of Efforts to Protect Hosting Centers	7
6. Disaster Recovery Plan	7
Effectiveness of Efforts to Control Access to the Data Exchange Gateway	9
8. DEG Security	9
Glossary of Acronyms and Terms	11

**DATA CENTER OPERATIONS
DEPARTMENT OF TECHNOLOGY, MANAGEMENT,
AND 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 Data Center Operations (DCO), Department of Information Technology (DIT) (084-0580-06), which was issued and distributed in July 2007. That audit report included 3 material conditions (Findings 1, 6, and 8) and 5 reportable conditions*.

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether the Department of Technology, Management, and Budget (DTMB) had taken appropriate corrective measures in response to the 3 material conditions and 4 corresponding recommendations.

BACKGROUND

DTMB's DCO provides centralized hosting services for all State of Michigan agencies. These services include the acquisition of hardware and software and operational and technical support for the State's mainframes and over 3,000 servers. In addition, DCO is responsible for monitoring system performance and recommending improvements in security, performance, and responsiveness to meet future computing demands in a timely manner.

* See glossary at end of report for definition.

Executive Order No. 2009-55 renamed the Department of Management and Budget (DMB) as the Department of Technology, Management, and Budget (DTMB), effective March 21, 2010. It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of the Department of Information Technology (DIT) to DTMB and abolished DIT.

SCOPE

Our fieldwork was conducted from June through August 2012. We interviewed DCO employees to determine the status of compliance with our recommendations. Also, we reviewed hosting center* and mainframe risk assessments*, disaster recovery plans for the hosting centers, the security plan and risk assessment for the State's data exchange gateway (DEG), and policies and procedures related to security over the DEG.

* See glossary at end of report for definition.

FOLLOW-UP RESULTS

EFFECTIVENESS* IN ADMINISTERING THE HOSTING CENTERS

RECOMMENDATION AND RESPONSE AS REPORTED IN JULY 2007:

1. Risk Assessments

RECOMMENDATIONS

We again recommend that DIT conduct a comprehensive risk assessment of hosting center operations.

We also again recommend that DIT perform risk assessments routinely or when systems, facilities, or other conditions change.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendations. DIT informed us that a plan has been developed by the Office of Enterprise Security to complete future internal risk assessments. The internal risk assessments are expected to be completed by October 2008. DCO will initiate a process to have external risk assessments performed every two years beginning in 2008.

FOLLOW-UP CONCLUSION

We concluded that DTMB had partially complied with these recommendations and that a reportable condition exists. Our follow-up disclosed:

- a. DTMB had partially complied with the recommendation as it related to part a. of the finding. DTMB contracted with a third party vendor that completed a Data Center Infrastructure Condition, Capacity and Risk Assessment analysis. However, the analysis focused on the physical and infrastructure* risks associated with the hosting centers and did not consider other operational functions, such as change management and environmental monitoring.

* See glossary at end of report for definition.

DTMB also contracted with another third party vendor that assessed the design of the internal control* for DCO and made recommendations for additional controls. This assessment included a review of the controls over some operational functions. However, although the control assessment is an important component of the risk assessment process, there are many other key components of a comprehensive risk assessment, such as a threat* and vulnerability* identification, an evaluation of the probability of occurrence, and an impact analysis. Therefore, until all key components are addressed, the hosting center risk assessment for operational functions is not complete or comprehensive in nature. This was also reflected by the vendor in its recommendation to DCO to implement additional controls to ensure that there is a formal risk assessment process for areas such as logical security.

- b. DTMB had complied with the recommendation as it related to part b. of the finding. DTMB completed risk assessments internally that considered the impact that natural disasters, neighboring hazards, hardware failures, or other factors could have on a facility's operations. In addition, DTMB contracted with a third party vendor that evaluated infrastructure condition for the hosting centers.
- c. DTMB had complied with the recommendation as it related to part c. of the finding. DTMB completed a security risk assessment for the Unisys* mainframe in April 2012. The Bull* mainframe is no longer in operation and, therefore, security risk assessments are not required.

EFFECTIVENESS OF EFFORTS TO PROTECT HOSTING CENTERS

RECOMMENDATION AND RESPONSE AS REPORTED IN JULY 2007:

6. Disaster Recovery Plan

RECOMMENDATION

We recommend that DIT develop and test disaster recovery plans for the hosting center facilities.

* See glossary at end of report for definition.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. As part of its existing hosting center processes, DIT informed us that it regularly performs, maintains, and updates several of the disaster recovery functions listed, including:

- A comprehensive inventory of all computer hardware, software, and support equipment in the Configuration Management Database.
- Vendor call and escalation lists.
- Emergency call lists for management and recovery teams.
- Copies of contracts and maintenance agreements.
- Processes for restoring or replacing support systems, such as power, air conditioning, and uninterruptible power supply.
- Generator power backup for all three hosting centers.

DIT informed us that it is continuing to expand recovery team duties and responsibilities to include all critical systems through its disaster recovery project. In addition, DIT will continue to work with DMB in completing procedures for securing a damaged site and will take the preceding information and create a disaster recovery plan for the hosting centers by the end of September 2008.

FOLLOW-UP CONCLUSION

We concluded that DTMB had partially complied with the recommendation and that a reportable condition exists. Our follow-up disclosed:

- DTMB had not fully documented all disaster recovery elements within the disaster recovery plans. We noted that DTMB had made significant progress in documenting most elements of the disaster recovery plans. However, we also noted some elements that were not documented within all of the plans, such as procedures for responding in the event of a disaster and equipment floor diagrams.

- DTMB had not performed testing of the disaster recovery plans for 2 of the 3 hosting centers. Because each of the hosting centers is significant to State operations, DTMB should ensure that the disaster recovery plans for all 3 hosting centers are properly tested and deemed satisfactory.

EFFECTIVENESS OF EFFORTS TO CONTROL ACCESS TO THE DATA EXCHANGE GATEWAY

RECOMMENDATION AND RESPONSE AS REPORTED IN JULY 2007:

8. DEG Security

RECOMMENDATION

We recommend that DIT fully implement security over the State's DEG.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT informed us that the security officer position was lost because of the 2001 early retirement. DIT was not granted authorization to replace the position until 2005. DIT informed us that it has developed a plan to complete implementation of security and the expected completion date is December 31, 2007.

FOLLOW-UP CONCLUSION

We concluded that DTMB had partially complied with the recommendation and that a material condition still exists. Our follow-up disclosed:

- a. DTMB had complied with the recommendation as it related to part a. of the finding. DTMB performed an information system security risk assessment for the DEG. The risk assessment identified potential threats and vulnerabilities, the risk if controls were not implemented, controls currently implemented, the probability of occurrence, and the potential impact and made recommendations for additional controls.

- b. DTMB had partially complied with the recommendation as it related to part b. of the finding. DTMB identified the recommended security requirements for the DEG based on its security level. However, in the security plan, DTMB did not describe specific controls in place to address a substantial number of the recommended security requirements. Until there is a clear relationship between the recommended security requirements and the controls in place that address those requirements, the security plan is not complete and there is an increased risk that DTMB will not implement necessary controls.

- c. DTMB had partially complied with the recommendation as it related to part c. of the finding. DTMB had not established all recommended policies and procedures governing the use of the DEG. For example, DTMB had not established policies and procedures that specified when agencies should use the DEG for data transfers, documented the roles and responsibilities of State agencies and DTMB for security, or defined how access was to be monitored and revoked. DTMB had developed draft policies and procedures that would further define some of these areas. However, the draft policies and procedures had not been formally approved or implemented.

- d. DTMB had not complied with the recommendation as it related to part d. of the finding. DTMB informed us that privileged accounts* are routinely monitored by a security specialist to identify unusual activity. However, DTMB could not provide system-generated data or other documentation to support management's assertion that privileged accounts were being routinely monitored.

* See glossary at end of report for definition.

Glossary of Acronyms and Terms

Bull	A mainframe computer manufacturer.
DCO	Data Center Operations.
DEG	data exchange gateway.
DIT	Department of Information Technology.
DMB	Department of Management and Budget.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Program success in achieving mission and goals.
hosting center	A State data center. A data center is a facility used to house computer systems and associated components.
infrastructure	In information technology and on the Internet, the physical hardware used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, cable television lines, and satellites and antennas, and also the routers, aggregators, repeaters, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals that are transmitted.
internal control	The organization, policies, and procedures adopted by management and other personnel to provide reasonable assurance that operations, including the use of resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws

and regulations are followed. Internal control also includes the safeguarding of assets against unauthorized acquisition, use, or disposition.

material condition A reportable condition that 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 economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.

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 individuals 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.

threat An activity, intentional or unintentional, with the potential for causing harm to an automated information system or activity.

Unisys A mainframe computer manufacturer.

vulnerability Weakness in an information system that could be exploited or triggered by a threat.

