MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

DATA CENTER OPERATIONS

DEPARTMENT OF INFORMATION TECHNOLOGY

July 2007

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

084-0580-06

> 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

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Data Center Operations

Department of Information Technology

Report Number:
084-0580-06

Released:
July 2007

The Department of Information Technology's (DIT's) Data Center Operations (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 2,000 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.

Audit Objective:
To assess DIT's effectiveness in administering the State's hosting centers.

Audit Conclusion:
DIT was moderately effective in administering the State's hosting centers. We noted one material condition (Finding 1) and four reportable conditions (Findings 2 through 5).

Material Condition:
DIT had not conducted a comprehensive risk assessment of hosting center operations. Also, DIT did not perform risk assessments routinely or when systems, facilities, or other conditions changed. (Finding 1)

Reportable Conditions:
DIT had not established an effective process for developing and managing service level agreements (Finding 2).

DIT had not developed a formal strategic plan and had not fully developed operational plans for its hosting center activities (Finding 3).

DIT had not developed formal return on investment and cost-benefit analyses to determine future hosting center alternatives (Finding 4).

DIT did not fully implement effective security practices for the Bull mainframe (Finding 5).

Noteworthy Accomplishments:
DIT has made significant progress in its server room consolidation project. Since 2004, DIT has closed 19 server rooms and migrated 273 servers into one of the State's hosting centers. The project also allowed DIT to salvage 310 servers. DIT informed us that the project includes the following benefits: improved availability of applications due to the increased reliability of the hosting center environment, cost savings from the elimination of hardware and server support costs, and cost avoidance of projected costs to upgrade

physical security and environmental controls at the server rooms to industry standards.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT’s efforts to protect the State's hosting centers from physical and environmental threats.

Audit Conclusion:
DIT's efforts to protect the State’s hosting centers from physical and environmental threats were moderately effective. We noted one material condition (Finding 6) and one reportable condition (Finding 7).

Material Condition:
DIT had not developed and tested disaster recovery plans for the hosting center facilities (Finding 6).

Reportable Condition:
DIT had not updated or fully developed policies and procedures governing physical security and environmental controls at the State’s hosting centers (Finding 7).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT's efforts to control access to the State's data exchange gateway (DEG).

Audit Conclusion:
DIT's efforts to control access to the State’s DEG were moderately effective. We noted one material condition (Finding 8).

Material Condition:
DIT had not fully implemented security over the State's DEG (Finding 8).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 8 findings and 9 corresponding recommendations. DIT's preliminary response indicates that it agrees with all of the recommendations and will comply with them.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

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

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

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

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

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

July 20, 2007

Ms. Teresa M. Takai, Director
Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Ms. Takai:

This is our report on the performance audit of Data Center Operations, Department of Information Technology.

This report contains our report summary; description of agency; audit objectives, scope, and methodology and agency responses and prior audit follow-up; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agency's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

DATA CENTER OPERATIONS
DEPARTMENT OF INFORMATION TECHNOLOGY

Page

INTRODUCTION

COMMENTS, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of Agency

The Department of Information Technology's (DIT's) Data Center Operations (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 2,000 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.

The major sections of DCO include:

a. Configuration Management

   Configuration Management plans for and facilitates the installation of equipment in the hosting centers*. In addition, Configuration Management supervises the removal of obsolete equipment from the hosting centers.

b. Enterprise Services

   Enterprise Services manages physical and environmental security at the hosting centers. The manager of Enterprise Services authorizes and reviews physical access to the hosting centers. Enterprise Services' Enterprise Monitoring group monitors the performance of hardware components located within the hosting centers.

   In addition, Enterprise Services' Service Management Center (SMC) provides daily briefings to other DIT organizations on significant information technology* events, such as outages, security events, and configuration changes. SMC assists in the communication and coordination of activities between DCO and the rest of DIT. SMC also participates in a change management board for DIT and the Department of State.

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

c. Enterprise Platform Services

Enterprise Platform Services provides technical support for the State's enterprise* platforms, including the Unisys* mainframe, Bull* mainframe, Teradata* data warehouse*, and the data exchange gateway. In addition, Enterprise Platform Services maintains third party utilities used by State agencies to manage scheduling, source codes, and files on the mainframes. Enterprise Platform Services also manages DCO's tape library.

d. Planning and Solutions Development

Planning and Solutions Development designs and manages the implementation of infrastructure* environments for systems hosted within DIT using release management processes based on the Information Technology Infrastructure Library (ITIL).

e. Scheduling and Data Entry Services

Scheduling and Data Entry Services schedules production jobs and provides data entry services for State agencies.

For fiscal year 2005-06, DCO had a budget of approximately $52.9 million with 68.5 full-time equated positions.

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

Audit Objectives, Scope, and Methodology and Agency Responses and Prior Audit Follow-Up

Audit Objectives

Our performance audit* of Data Center Operations (DCO), Department of Information Technology (DIT), had the following objectives:

1. To assess DIT's effectiveness* in administering the State's hosting centers.

2. To assess the effectiveness of DIT's efforts to protect the State's hosting centers from physical and environmental threats.

3. To assess the effectiveness of DIT's efforts to control access to the State's data exchange gateway (DEG).

Audit Scope

Our audit scope was to examine the information processing and other records related to controls over Data Center Operations. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances. Our audit procedures, performed from July 2006 through January 2007, generally covered the period March 2004 through January 2007.

Audit Methodology

The criteria used in the audit included control objectives and audit guidelines outlined in the Control Objectives for Information and Related Technology* (COBIT) issued by the Information Systems Audit and Control Foundation (ISACF) in July 2000, guidelines issued by the National Institute of Standards and Technology (NIST), and other

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

information security and industry best practices. To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase
   We conducted a preliminary review to obtain an understanding of DCO. We interviewed DCO management to obtain an understanding of each section's roles and responsibilities. We obtained and reviewed DIT's policies and procedures for data center administration, physical and environmental security, and the DEG. We obtained an understanding of the risks associated with the hosting centers. We used the results of our review to determine the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase
   We performed an assessment of DIT's efforts to administer the hosting centers and an assessment of the effectiveness of DIT's efforts to protect hosting centers from physical and environmental threats. We also assessed the effectiveness of DIT's efforts to control access to the DEG:

   a. DIT's Effectiveness in Administering the Hosting Centers:

      (1) We reviewed DIT's strategic planning process for hosting center operations.

      (2) We evaluated the content of service level agreements* between DIT and State agencies.

      (3) We evaluated DIT's risk assessments of hosting center operations.

      (4) We assessed DIT's efforts to comply with select prior audit recommendations related to the security over mainframes.

   b. Effectiveness of DIT's Efforts to Protect Hosting Centers:

      (1) We assessed DCO's physical security and environmental controls at each of the hosting centers.

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

(2) We reviewed DCO's policies and procedures for implementing physical security and environmental controls. In addition, we assessed DCO's procedures for testing and maintaining hosting center equipment, such as backup generators and air conditioners.

(3) We reviewed and evaluated DCO's risk assessments for the hosting centers.

c. Effectiveness of DIT's Efforts to Control Access to the DEG:

(1) We interviewed DCO management to obtain an understanding of the DEG system architecture.

(2) We reviewed DCO's policies and procedures governing the use of the DEG.

(3) We assessed DCO's activities to ensure that only authorized users have access to files on the DEG.

(4) We assessed DCO's actions to monitor the activities of DEG system administrators.

3. Evaluation and Reporting Phase

We evaluated and reported on the results of the detailed analysis and testing phase.

We use a risk and opportunity based approach when selecting activities or programs to be audited. Accordingly, our audit efforts are focused on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. By design, our limited audit resources are used to identify where and how improvements can be made. Consequently, our performance audit reports are prepared on an exception basis. To the extent practical, we add balance to our audit reports by presenting noteworthy accomplishments for exemplary achievements identified during our audits.

Agency Responses and Prior Audit Follow-Up

Our audit report contains 8 findings and 9 corresponding recommendations. DIT's preliminary response indicates that it agrees with all of the recommendations and will comply with them.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require DIT to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

Within the scope of this audit, we followed up 8 of the 9 audit recommendations from our December 1998 performance and financial related audit of the Michigan Information Processing Center (MIPC), Department of Management and Budget (07-595-97). With the establishment of DIT, MIPC became DCO. DCO complied with 3 of the prior audit recommendations, 2 prior audit recommendations were repeated, and the other 3 were rewritten for inclusion in this report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS IN ADMINISTERING THE HOSTING CENTERS

COMMENT

Audit Objective: To assess the Department of Information Technology's (DIT's) effectiveness in administering the State's hosting centers.

Conclusion: DIT was moderately effective in administering the State's hosting centers. Our assessment disclosed one material condition*:

- DIT had not conducted a comprehensive risk assessment* of hosting center operations. Also, DIT did not perform risk assessments routinely or when systems, facilities, or other conditions changed. (Finding 1)

Our assessment also disclosed four reportable conditions* regarding service level agreements, strategic and operational planning, hosting center alternatives, and Bull mainframe security (Findings 2 through 5).

Noteworthy Accomplishments: DIT has made significant progress in its server room consolidation project. Since 2004, DIT has closed 19 server rooms and migrated 273 servers into one of the State's hosting centers. The project also allowed DIT to salvage 310 servers. DIT informed us that the project includes the following benefits: improved availability of applications due to the increased reliability of the hosting center environment, cost savings from the elimination of hardware and server support costs, and cost avoidance of projected costs to upgrade physical security and environmental controls at the server rooms to industry standards.

FINDING

1. Risk Assessments

DIT had not conducted a comprehensive risk assessment of hosting center operations. Also, DIT did not perform risk assessments routinely or when systems, facilities, or other conditions changed. As a result, DIT cannot ensure that significant risks have been identified and that appropriate cost-effective safeguards have been incorporated into its activities.

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

Our review of risk assessments for hosting center operations disclosed:

a. DIT had not performed a risk assessment for all operational functions of hosting center operations. DIT policy 100.15 requires each organizational unit in DIT to develop and complete a regular assessment of business risks and prepare a plan for reducing the risks to an acceptable level. In 2004, DIT contracted for a risk assessment of the hosting centers. However, to comply with policy 100.15, the risk assessment should be expanded to include other Data Center Operations (DCO) functions, such as change management, environmental monitoring, and technical support.

b. DIT's risk assessments of the hosting centers did not fully consider all significant risks to the hosting centers. In addition to the risk assessment contracted by DIT, DIT participated in three physical security risk assessments performed by the Department of Management and Budget (DMB) in response to its Continuation of Government project. However, the risk assessments focused primarily on environmental controls, such as utilities, air conditioning, and fire suppression, as well as physical security controls. A more comprehensive risk assessment may consider the impact that natural disasters, neighboring hazards, hardware failures, internal procedures, a security program, and contingency planning could have on a facility's operation.

c. DIT had not updated its security risk assessments for the State's Unisys and Bull mainframes since 2000. Because risk assessments are for a specific time period in a continuously changing environment, the National Institute of Standards and Technology (NIST) suggests that agencies perform risk assessments every three years or when systems, facilities, or other conditions undergo significant change.

This finding was reported in our December 1998 performance and financial related audit of the Michigan Information Processing Center (MIPC), Department of Management and Budget (07-595-97). MIPC stated that it would conduct risk assessments for each of its mainframes, including a review of physical security at the hosting centers by June 30, 1999. Although MIPC completed risk assessments for the mainframes in 2000, DIT had not performed ongoing risk assessments because of the early retirement of the mainframe security officers in November

2002. DIT did not receive authorization to hire replacement security officers until October 2005.

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.

FINDING

2. Service Level Agreements

DIT had not established an effective process for developing and managing service level agreements (SLAs). As a result, the SLAs did not contain sufficient detail to improve operational efficiencies and customer satisfaction.

The purpose of an SLA is to define the relationship between and the responsibilities and expected performance of DIT and the State agencies that DIT serves. Effective SLAs would improve DIT's ability to ensure that agencies' information processing objectives are met, customer expectations are managed, and customer satisfaction is achieved. Executive Order No. 2001-3 required DIT to establish SLAs with executive branch departments and agencies.

We reviewed DIT's SLA template and DIT's SLAs with the Department of Treasury and the Department of Human Services. Our review disclosed:

a. The SLAs did not describe the specific services provided by DIT. For example, the SLAs did not explain the services offered by DCO and did not document the level of support that DCO will provide for systems housed in each of the hosting centers. In addition, the SLAs did not identify the actual services purchased by each State agency. This lack of detail increases the likelihood of misunderstandings between DIT and State agencies regarding the services the agencies believe they are purchasing from DIT and the actual services DIT is providing.

b. The SLAs and other supporting documentation did not describe the services that an agency could expect to receive as part of DIT's pricing. In addition, the pricing documentation did not include prices for other services, such as security, contract, and procurement services. The SLA directs agencies to a rate schedule posted on DIT's Intranet; however, the rate schedule did not provide sufficient detail. Providing detailed price information could assist State agencies in managing costs and making choices about information technology (IT) services.

c. The SLAs included metrics* for system performance, such as application availability* or time to restore service, that DIT did not have the ability to measure and that were developed without sufficient involvement from DCO. DIT informed us that it is in the process of determining if the metrics are measurable, identifying the resources needed to measure the metrics, and determining how to collect the data to measure the baseline metrics.

   Establishing and reporting on system performance metrics would provide evidence that DIT is successfully meeting the requirements of its customers. Also, according to the Control Objectives for Information and Related Technology (COBIT), the parties responsible for the performance being measured should be fully involved in the development of the metrics.

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

RECOMMENDATION

We recommend that DIT establish an effective process for developing and managing SLAs.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT informed us that SLAs have been updated and improved since the audit took place as part of the ongoing strategic management team SLA initiative. The Office of the Auditor General recommendations will be included as enhancements to the fiscal year 2007-08 SLAs.

FINDING

3. Strategic and Operational Planning

DIT had not developed a formal strategic plan and had not fully developed operational plans for its hosting center activities. The lack of strategic and operational plans diminishes DCO's ability to ensure that its activities are properly aligned with DIT's IT strategic plan and State agencies' business requirements in a planned and cost-effective manner.

Strategic planning is the long-term process of assessment, goal-setting, and decision-making for future operations. A strategic plan defines what an organization seeks to accomplish and identifies the strategies it will use to achieve the desired results. Furthermore, a strategic plan is the starting point for an organization's performance measurement efforts.

Operational plans translate the objectives and high level strategies of the strategic plan into operational strategies, objectives, and actions, with assigned responsibilities and performance indicators. The purpose of strategic and operational planning is to ensure that all planning is coordinated and integrated with other organizational processes, including budget development and resource allocation.

In September 2006, DCO held a strategic planning workshop to discuss the State's future computing and disaster recovery needs. In addition, DCO developed a high level plan for upgrading the hosting centers. However, these activities did not result in formal strategic and operational plans approved by DIT's executive management. Because DCO is responsible for a significant portion of the State's IT infrastructure, it is vitally important that DIT and DCO fully develop and implement plans to ensure that the infrastructure can support the State's future business needs.

DIT had not developed formal plans for hosting center activities because DIT had not established formal policies and procedures requiring its organizational units to develop and maintain strategic and operational plans for their significant business activities. COBIT recommends that organizations engage in strategic planning processes to obtain a favorable balance between IT opportunities and business requirements.

RECOMMENDATION

We recommend that DIT develop a formal strategic plan and fully develop operational plans for its hosting center activities.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT agrees that a tighter focus on infrastructure planning could add tremendous value to its current process. DIT informed us that the strategic management team annually reviews and approves the hosting center budget and proposes initiatives and goals for alignment with DIT's strategic plan and the Governor's cabinet action plan. DIT informed us that it will document the results of this planning process by September 2008 with the development of an infrastructure services strategic plan.

FINDING

4. Hosting Center Alternatives

DIT had not developed formal return on investment* (ROI) and cost-benefit analyses* to determine future hosting center alternatives. Such analyses would be helpful in identifying opportunities to improve operational efficiencies and in identifying the associated risks to the State.

To reduce support costs and improve service and security, DIT began consolidating State agencies' servers into the hosting centers. However, DIT did

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

not complete a cost-benefit analysis that included an assessment of the associated risks of the consolidations. Although the consolidation strategy gives DIT the potential to achieve greater operating efficiencies and long-term cost savings, the consolidations have also increased the State's risk in the event of a hosting center disaster.

DIT informed us that it adopted the Information Technology Infrastructure Library's (ITIL's) best practices for delivering services more effectively and efficiently. ITIL identified security management, change management, capacity management, and availability management as examples of key areas in which improvements in hosting center operations may result in cost savings. Our review disclosed the following examples of areas that DIT should consider while developing future hosting center strategies:

a. DIT's hosting centers have physical security and environmental control weaknesses that cannot be corrected because of the hosting center's location or cannot be corrected without significant investment. When DMB consolidated the State's mainframes in 1994, it selected the current location of the hosting centers. However, neither DIT nor DMB could provide us with evidence that a risk assessment was performed that considered physical and environmental risks when DMB made the site selection.

b. The cost of improving system availability and future server expansion may be an inefficient use of resources in the long term. DIT indicated that it would like to achieve an Uptime Institute Tier III* rating standard of 99.982% systems availability at the hosting centers. However, DIT estimated that achieving this standard will cost approximately $39 million. Given the cost of upgrades and renovations, DIT should further study whether it would be more cost effective to replace rather than upgrade the hosting centers.

c. Because of the direct relationship between the number of servers and the amount of support costs, server utilization is a potential area in which DIT could achieve cost savings. A 2004 risk assessment reported that State agencies are traditionally placing only one application on each server.

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

Industry best practices indicate that a server typically supports multiple applications. The risk assessment estimated that the State could potentially eliminate 600 (38%) of its 1,600 production servers. In January 2007, DIT completed its consolidation of the State's e-mail systems and consolidated 40 systems down to 2 systems for projected cost savings of $11 million over the next four years. Where feasible, further consolidation of servers would assist DIT in optimizing the State's infrastructure resources.

RECOMMENDATION

We recommend that DIT develop formal ROI and cost-benefit analyses to determine future hosting center alternatives.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT informed us that it has completed a comprehensive ROI analysis for current server room consolidation activities and will continue to plan and analyze financial and security implications for future data center initiatives. When DIT receives approval for initial funding, the in-depth study will include detailed planning, ROI, and cost-benefit analyses. DIT expects to complete the planning process approximately 6 to 9 months after the funding is approved by the Office of the State Budget.

FINDING

5. Bull Mainframe Security

DIT had not fully implemented effective security practices for the Bull mainframe. Without fully implemented security practices, DIT cannot ensure that the Bull mainframe has been properly secured and controls are functioning as intended.

We followed up on security weaknesses first reported in our December 1998 performance and financial related audit of Michigan Information Processing Center, Department of Management and Budget (07-595-97), for which DIT is now responsible. Our review disclosed that DIT had not remediated the following weaknesses:

a. DIT had not established an audit trail of changes to the Bull mainframe operating system.

b. DIT did not monitor computer console activities.

c. DIT did not monitor the activities of its privileged users or the use of privileged programs.

When the security officer for the Bull mainframe retired in 2001, DIT was not granted authorization to fill the position. In October 2005, DIT hired a security officer for the Bull mainframe. Although the security officer was working with DIT to remediate the weaknesses, we noted that the security officer did not have prior knowledge or experience with the Bull mainframe operating system to effectively implement changes. We also noted that DIT had not updated security procedures to include all of the security officer's activities. Formally documenting security procedures would help DIT ensure the continuation of security practices in the event of a personnel change.

RECOMMENDATION

We recommend that DIT fully implement effective security practices for the Bull mainframe.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT informed us that it has developed a plan to complete implementation of security by December 2007.

EFFECTIVENESS OF EFFORTS TO PROTECT HOSTING CENTERS

COMMENT

Audit Objective: To assess the effectiveness of DIT's efforts to protect the State's hosting centers from physical and environmental threats.

Conclusion: DIT's efforts to protect the State's hosting centers from physical and environmental threats were moderately effective. Our assessment disclosed one material condition. DIT had not developed and tested disaster recovery plans for the hosting center facilities (Finding 6). Our assessment also disclosed one reportable condition regarding policies and procedures (Finding 7).

FINDING

6. Disaster Recovery Plan

DIT had not developed and tested disaster recovery plans for the hosting center facilities. The lack of disaster recovery plans decreases the likelihood that the State's information systems could be restored in a timely, cost-effective manner.

COBIT requires organizations to establish documented disaster recovery and business continuity plans to lessen the impact of a service interruption. Disaster recovery plans for facilities such as the hosting centers should include:

- Comprehensive inventory of all computer hardware, software, and support equipment.
- Vendor call and escalation lists.
- Emergency call lists for management and recovery teams.
- Recovery team duties and responsibilities.
- Equipment room floor grid diagrams.
- Copies of contracts and maintenance agreements.
- Procedures for securing the damaged site.
- Procedures for restoring or replacing support systems, such as power, air conditioning, and uninterruptible power supply.

DIT has documented some disaster recovery plan elements and has made efforts to reduce the impact of a disaster. During our audit fieldwork, DCO informed us that it was in the process of completing an inventory of equipment and was updating its configuration database. In addition, for some critical agency systems, DIT provides disaster recovery solutions, such as the automatic mirroring of systems at its backup hosting center. DIT also informed us that it is in the process of updating and testing its disaster recovery plans for the State's mainframes.

RECOMMENDATION

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

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.

FINDING

7. Policies and Procedures

DIT had not updated or fully developed policies and procedures governing physical security and environmental controls at the State's hosting centers. Without updated policies and procedures, DIT cannot ensure that the hosting centers are in compliance with current standards and industry best practices.

For example:

a. DIT had not updated DMB Administrative Guide procedure 1310.02, which defines physical security and environmental control requirements for the hosting centers. DCO informed us that DIT intended to operate the State's hosting centers at Tier III as defined by the Uptime Institute. DCO also informed us that it follows other standards, such as those of the National Fire Protection Association. However, DIT had not updated procedure 1310.02 to include these standards.

b. DIT had not established minimum physical security and environmental control standards for information systems located outside of the hosting centers. According to DIT's SLAs with State agencies, DIT is responsible for general controls over the State's information systems. As such, DIT should establish standards to ensure that information systems are properly protected.

c. DIT had not established a Statewide exit interview policy requiring State agencies to notify DIT when an employee or contractor departs or no longer requires access to a hosting center. DIT relies on State agencies to inform it when access is no longer required. The lack of a formal policy for notifying DIT increases the risk that an individual's access may not be revoked in a timely manner.

RECOMMENDATION

We recommend that DIT update and fully develop policies and procedures governing physical security and environmental controls at the State's hosting centers.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the recommendation and informed us that it has begun updating the appropriate DMB Administrative Guide policies and procedures. DIT expects to publish updated policies and procedures by June 2008.

EFFECTIVENESS OF EFFORTS TO CONTROL ACCESS TO THE DATA EXCHANGE GATEWAY

COMMENT

Background: The State's data exchange gateway (DEG) was established to provide a single, secure point of access and data file transfer between the State's business partners and systems hosted on one of the State's mainframes. The DEG now also provides data transfer services for other systems, such as the State's data warehouse. The DEG transfers approximately 720,000 data files each year. Many of the files contain confidential data, such as social security numbers, medical records, and financial data.

Audit Objective: To assess the effectiveness of DIT's efforts to control access to the State's DEG.

Conclusion: DIT's efforts to control access to the State's DEG were moderately effective. Our assessment disclosed one material condition. DIT had not fully implemented security over the State's DEG (Finding 8).

FINDING

8. DEG Security

DIT had not fully implemented security over the State's DEG. As a result, DIT could not ensure that the DEG was protected from unauthorized access.

Our review of DIT's efforts to control access to the DEG disclosed:

a. DIT had not performed an information system security risk assessment for the DEG. An information system security risk assessment is necessary to ensure that security threats and vulnerabilities are identified and to determine the effectiveness of current or proposed controls. For example, the risk assessment should identify areas of vulnerability related to personnel, facilities, hardware, system software, operating systems, and applications. DIT should assess risks posed by both authorized and unauthorized users trying to access the DEG.

b. DIT had not developed a security plan for the DEG. Without a security plan, DIT cannot ensure that DEG security requirements are appropriately addressed. The purpose of a security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.

c. DIT had not established policies and procedures governing the use of the DEG. For example, DIT did not have policies or procedures that:

- Specified when agencies must use the DEG for data transfers.
- Documented the roles and responsibilities of State agencies and DIT for security and disaster recovery.

- Specified security measures, such as encryption, that must be implemented based on the confidentiality of data.
- Defined how access is to be granted, revoked, and monitored.

Documented policies and procedures would help DIT ensure that the DEG is consistently managed and secured in accordance with management's intent.

d. DIT did not monitor the activities performed with privileged accounts. Privileged accounts have the ability to override security and controls. Therefore, activities performed with privileged accounts should be identified, logged, and monitored by management.

DIT had taken some steps to secure the DEG. DIT routinely performed vulnerability scans of the DEG and, in November 2005, DIT hired a security officer whose responsibilities include security of the DEG. However, at the time of our review, the security officer had not conducted any security reviews of the DEG.

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.

GLOSSARY

Glossary of Acronyms and Terms

availability	Timely and reliable access to data and information systems.
Bull	A mainframe computer manufacturer.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines developed by the Information Systems Audit and Control Foundation (ISACF) as a generally applicable and accepted standard for good practices for controls over information technology.
cost-benefit analysis	The process of weighing expected costs against expected benefits to determine the best (or most profitable) course of action.
data warehouse	A very large database designed for fast processing of queries, projections, and data summaries, normally used by a large organization.
DCO	Data Center Operations.
DEG	data exchange gateway.
DIT	Department of Information Technology.
DMB	Department of Management and Budget.
effectiveness	Program success in achieving mission and goals.
enterprise	An organization. In the context of this audit report, "enterprise" encompasses DIT and all other State agencies that run information systems on the State's network.

hosting center

A State data center. A data center is a facility used to house computer systems and associated components.

information technology (IT)

Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources.

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.

ITIL

Information Technology Infrastructure Library.

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.

metrics

Measurements designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

MIPC

Michigan Information Processing Center.

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.

reportable condition

A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.

return on investment (ROI)

The amount of profit or cost savings realized for a given use of money in an enterprise. An ROI calculation is sometimes used along with other approaches to develop a business case for a given proposal. The overall ROI for an enterprise is sometimes used as a way to grade how well a company is managed.

risk assessment

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

service level agreement (SLA)

A written agreement between the provider of a service and the customer(s) that documents the agreed service levels for the service.

SMC

Service Management Center.

Teradata

A computer manufacturer. Teradata is a software company, founded in 1979, that develops and sells a relational database management system with the same name.

Tier III

The Uptime Institute's classification system for infrastructure site availability. A Tier III level allows for any planned site infrastructure activity without disrupting the computer hardware operation.

Unisys

A mainframe computer manufacturer.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

STATE OF MICHIGAN · OFFICE of the AUDITOR GENERAL ·