MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

UNISYS MAINFRAME GENERAL CONTROLS

MICHIGAN DEPARTMENT OF INFORMATION TECHNOLOGY

January 2010

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

084-0550-09

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

Unisys Mainframe General Controls

Michigan Department of Information Technology

Report Number:
084-0550-09

Released:
January 2010

Unisys mainframe computers store and process critical State systems and data to support important government services, including licensing drivers and motor vehicles, processing income and business tax collections and returns, and maintaining prisoner records. The Michigan Department of Information Technology (MDIT) is responsible for the operation, security, and technical support of the mainframes. Protecting the integrity and confidentiality of data stored on the mainframes is accomplished through the implementation of information technology general controls.

Audit Objective:
To assess the effectiveness of MDIT's access controls over the State's mainframe information systems.

Audit Conclusion:
MDIT's access controls over the State's mainframe information systems were moderately effective. We noted three reportable conditions (Findings 1 through 3).

Reportable Conditions:
MDIT had not established sufficient access controls over the Unisys mainframe computers (Finding 1).

MDIT had not established effective security controls over critical Unisys mainframe computer files (Finding 2).

MDIT did not effectively manage and monitor the use of BL/Source and BL/Sched software products (Finding 3).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of MDIT's efforts in establishing physical and environmental controls over the State's mainframe information systems.

Audit Conclusion:
MDIT's efforts in establishing physical and environmental controls over the State's mainframe information systems were moderately effective. We noted one reportable condition (Finding 4).

Reportable Condition:
MDIT had not established effective access controls to the computer facilities that house the Unisys mainframe computers (Finding 4).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of MDIT's efforts in establishing appropriate backup and disaster recovery controls over the State's mainframe information systems.

Audit Conclusion:
MDIT's efforts in establishing appropriate backup and disaster recovery controls over the State's mainframe information systems were moderately effective. We noted one reportable condition (Finding 5).

Reportable Condition:
MDIT had not established sufficient backup and disaster recovery processes (Finding 5).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 5 findings and 5 corresponding recommendations. MDIT'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

January 20, 2010

Mr. Kenneth D. Theis, Director
Michigan Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Mr. Theis:

This is our report on the performance audit of Unisys Mainframe General Controls, Michigan Department of Information Technology.

This report contains our report summary; description of agency; audit objectives, scope, and methodology and agency responses; 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

UNISYS MAINFRAME GENERAL CONTROLS
MICHIGAN DEPARTMENT OF INFORMATION TECHNOLOGY

Description of Agency

Data Center Operations* (DCO), Michigan Department of Information Technology (MDIT), is responsible for managing the central computer facilities which house some of the State's most critical systems and data. These systems help the State departments deliver important government services, including:

- Licensing drivers and motor vehicles.
- Processing income and business tax collections and returns.
- Processing mental health facility billings.
- Maintaining the workers' compensation program.
- Maintaining prisoner records.

These systems and their data are stored and processed on Unisys mainframe computers*. DCO is responsible for the operation, security, and technical support of the mainframes. As of August 2009, five departments had systems on the mainframes.

Protecting the integrity and confidentiality of data stored on the mainframes is accomplished through the implementation of information technology* general controls. These controls include access controls to prevent unauthorized persons from viewing or modifying programs or data, physical and environmental security of the mainframe hardware, and backup and disaster recovery controls to help ensure recovery of programs and data in the event of a disaster.

Mainframe security, including user access rights and file security, is a shared responsibility between MDIT and the departments using the mainframes. DCO uses a complex security system to control access to mainframe resources. The security system uses a decentralized approach to security which allows department security administrators* to define authorized individuals and grant appropriate access to information resources.

MDIT Agency Services is responsible for providing application development, maintenance, and database management. Information system security is a shared responsibility among DCO, Agency Services, and the departments using the mainframes.

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

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of Unisys Mainframe General Controls, Michigan Department of Information Technology (MDIT), had the following objectives:

1. To assess the effectiveness* of MDIT's access controls over the State's mainframe information systems.

2. To assess the effectiveness of MDIT's efforts in establishing physical and environmental controls over the State's mainframe information systems.

3. To assess the effectiveness of MDIT's efforts in establishing appropriate backup and disaster recovery controls over the State's mainframe information systems.

Audit Scope

Our audit scope was to examine the information processing and other records related to general controls over the Unisys mainframe computers. 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. Our audit procedures, conducted from May through August 2009, generally covered the period October 2008 through August 2009.

Audit Methodology

We conducted a preliminary review of the general controls over the mainframes to obtain an understanding of mainframe access, computer operations, backup and recovery, disaster recovery, physical security, change management, and BL/Source* and BL/Sched* software access. We used the results of our preliminary review to determine the extent of our detailed analysis and testing.

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

To accomplish our first objective, we obtained an understanding of policies and procedures regarding access to the mainframes, selected change management software, and selected computer operations software. We interviewed MDIT staff and reviewed MDIT policies, procedures, and mainframe documentation to obtain an understanding of user access. We reviewed and assessed user authorization and password controls over the mainframes. We also examined and tested privileged user accounts. We reviewed mainframe documentation to obtain an understanding of high-risk access rights. We judgmentally selected 2 of the 5 departments that have systems on the mainframe which represented the primary users of the mainframes to examine and test access rights. We judgmentally selected and reviewed access rights which granted users the ability to perform high-risk functions on the mainframes.

In addition, we examined and reviewed file access rights over selected department files. We judgmentally selected 2 of the 5 departments to review file access rights. We identified the departments' pack families* and judgmentally selected 6 (33%) of 18 pack families for the first department, 2 (33%) of 6 pack families for the second department, and 16 (33%) of 49 pack families for the Unisys mainframe operating system to assess the pack family security settings. Further, we reviewed and assessed MDIT's monitoring of mainframe access and security.

We reviewed and assessed user authorization, user access rights, and password controls over BL/Source and BL/Sched software. We interviewed MDIT staff and reviewed software documentation to obtain an understanding of high-risk access rights. We judgmentally selected the same 2 departments as selected for our review of mainframe access rights to review BL/Source and BL/Sched access rights. We judgmentally selected and reviewed access rights which granted users the ability to perform high-risk change management or computer operations functions. We reviewed and assessed MDIT's monitoring of selected change management and computer operations software access and security.

To accomplish our second objective, we interviewed MDIT staff and reviewed policies and procedures to obtain an understanding of physical and environmental controls at the computer facilities that house the mainframes. We toured and assessed physical and environmental controls at the computer facilities that housed the mainframes.

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

To accomplish our third objective, we interviewed MDIT staff and reviewed policies and procedures to obtain an understanding of backup and disaster recovery controls. We reviewed mainframe backup and disaster recovery processes. We did not review and assess the completeness and effectiveness of the mainframe or computer room disaster recovery plans.

When selecting activities or programs for audit, we use an approach based on assessment of risk and opportunity for improvement. Accordingly, we focus our audit efforts on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. Our limited audit resources are used, by design, to identify where and how improvements can be made. Consequently, we prepare our performance audit reports on an exception basis.

Agency Response

Our audit report contains 5 findings and 5 corresponding recommendations. MDIT'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 the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require MDIT to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

ACCESS CONTROLS

COMMENT

Audit Objective: To assess the effectiveness of the Michigan Department of Information Technology's (MDIT's) access controls over the State's mainframe information systems.

Audit Conclusion: MDIT's access controls over the State's mainframe information systems were moderately effective. Our assessment disclosed three reportable conditions* regarding mainframe access controls, mainframe file security, and BL/Source and BL/Sched software access controls (Findings 1 through 3).

FINDING

1. Mainframe Access Controls

MDIT had not established sufficient access controls over the Unisys mainframe computers. Without sufficient access controls, MDIT cannot ensure the availability, integrity, and confidentiality of the State's information systems and data.

Federal Information System Controls Audit Manual (FISCAM) states that access controls help limit or detect inappropriate access to computer resources, thereby protecting mainframe programs and data from unauthorized modification, loss, and disclosure.

Mainframe access controls are a shared responsibility among MDIT's Data Center Operations (DCO), Agency Services, and the departments using the mainframes. DCO establishes password controls, monitors for high-risk activity, and grants administrative access rights. Agency Services and the departments grant access rights to users.

We reviewed selected high-risk access rights for users at MDIT and 2 of the 5 departments. Our review of access rights and password controls over the mainframes disclosed:

a. MDIT, in conjunction with the departments, did not develop policies and procedures that define the risks associated with granting certain high-risk

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

access rights and who should be granted these rights. For example, high-risk access rights allow users to copy and/or remove critical production files. We noted that MDIT and the 2 departments granted 101 users these high-risk access rights. Although MDIT and 1 of the departments implemented controls to monitor high-risk user activity, a preventive control such as defining and limiting access rights is a more effective control. FISCAM states that privileged access* is only appropriate for a limited number of users.

b. MDIT and the 2 departments granted developers unnecessary access to production program files and data. Granting development staff access to production files and data creates a risk that unauthorized changes to programs and data could be made because of the development staff's detailed understanding of the programs and controls. Although MDIT and 1 of the 2 departments monitored the developers' access to production files and data to ensure developers' activity was appropriate, a preventative control such as limiting developers access to production files and data is a more effective control.

c. MDIT and 1 of the 2 departments did not periodically review mainframe users' access rights to ensure their appropriateness. Control Objectives for Information and Related Technology* (CobiT) states that regular reviews of user accounts and related access rights help to ensure that only authorized users are accessing and using the mainframe resources and data.

d. Overall, MDIT and the 2 departments did not document and maintain proper authorization of the access rights assigned to users. We noted:

   (1) MDIT and 1 of the departments did not require and maintain any user access request forms.

   (2) MDIT and the other department did not completely maintain user access request forms. We determined that 3 (12%) of 26 users did not have access request forms documenting authorization for all access rights granted to the user. After bringing this matter to the department's

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

attention, MDIT and the department created the access request forms and obtained proper authorization for the 3 users.

Overall, establishing a process to approve and document assigned access rights helps to ensure that only authorized users have access to department systems and data.

e. MDIT did not completely implement strong password controls. We reviewed mainframe password settings and noted that MDIT did not configure the mainframe to require users' passwords to be a strong minimum password length and contain a combination of alphanumeric and special characters. Department of Management and Budget (DMB) Administrative Guide procedure 1410.17 states that passwords should be a minimum of 6 to 8 characters and contain a combination of alphanumeric and special characters. Without strong password controls, MDIT cannot ensure the security and integrity of systems and data.

Although our review only included mainframe access controls over MDIT and 2 departments, MDIT, in conjunction with the departments, should strengthen its mainframe access controls over the entire mainframe environment.

RECOMMENDATION

We recommend that MDIT establish sufficient access controls over the Unisys mainframe computers.

AGENCY PRELIMINARY RESPONSE

MDIT agrees and will comply with the recommendation.

With regard to part a., MDIT informed us that, by November 2010, it will develop a policy to define the risks associated with granting high-risk access rights and to define who should be granted these rights for this platform.

With regard to part b., MDIT informed us that it will review the process of granting developers access to production applications and data and that, by November 2010, it will develop a policy to limit and control this access.

With regard to part c., MDIT informed us that it will perform an analysis of its access rights review process by March 2010 and ensure that, by November 2010, the department's security administrators and the agency security administrators are performing periodic and thorough reviews to ensure the safety of the Unisys systems and data.

With regard to part d., MDIT informed us that, by March 2010, it will create a user access request form and that access will only be granted with an authorized agency requestor's approval. Those forms will be maintained in a central hard copy file within DCO.

With regard to part e., MDIT informed us that it supports strong passwords in accordance with Internal Revenue Service and DMB Administrative Guide procedures. MDIT also informed us that it will meet this strong password requirement as appropriate by November 2010.

FINDING

2. Mainframe File Security

MDIT had not established effective security controls over critical Unisys mainframe computer files. Without effective access controls, mainframe files may be viewed or modified by unauthorized users.

State departments store thousands of files on the mainframe computer. MDIT and departments control access to these files by assigning security attributes to files. Security attributes define the access granted to privileged and nonprivileged users. For example, one security attribute allows only privileged users to have direct access to the files. The appropriate security attributes depend on the access level that is required and the confidential or critical nature of the file. The security attributes assigned to the file can be changed by certain users who have access to the file.

Each department that uses the mainframes is assigned space on the mainframe called "pack families" for storing their applications and data. Also, MDIT uses packs called overhead packs to store files such as the system software, code files, security programs, and utility programs. These files ensure the proper functioning and security of the mainframes. MDIT and the departments are responsible for the security of departments' packs and MDIT is responsible for the security of overhead packs. We reviewed security attributes assigned to packs for MDIT and 2 of the 5 departments that have systems on the mainframe. We reviewed one third (33%) of the packs for each of the 2 departments. We also reviewed the security attributes for one third (33%) of the overhead packs. We noted:

a. MDIT and 1 of the 2 departments did not consistently complete periodic reviews of the security attributes for its packs. Periodic reviews of security attributes help to ensure that files are properly secured from unauthorized access. If files are not properly secured, sensitive data or critical application programs could be inappropriately modified or viewed.

b. MDIT did not consistently complete periodic reviews of the security attributes for the overhead packs. We noted that mainframe users had read and write access to 31% of the overhead files. Although the read and write access granted to these overhead files may be appropriate for some users, MDIT should periodically review the security attributes to ensure that overhead packs are properly secured.

DMB Administrative Guide procedure 1310.02 requires that production files be protected from unauthorized access. MDIT should establish a process to periodically review file security attributes to ensure that all critical and confidential files are identified and properly secured.

Although our review only included mainframe file security controls over MDIT and 2 departments, MDIT, in conjunction with the departments, should strengthen its mainframe file security controls over the entire mainframe environment.

RECOMMENDATION

We recommend that MDIT establish effective security controls over critical Unisys mainframe computer files.

AGENCY PRELIMINARY RESPONSE

MDIT agrees and informed us that it will establish effective security controls over critical Unisys mainframe computer files. MDIT informed us that it will provide department security administrators with the security attributes of all pack families every 12 months. Agency Services will review and document any changes needed. Those changes will be reviewed by the Office of Enterprise Security (OES) prior to adjustments being made to security settings. In addition, MDIT informed us that security attributes of all overhead pack families will be reviewed and adjusted annually by DCO and OES.

FINDING

3. BL/Source and BL/Sched Software Access Controls

MDIT did not effectively manage and monitor the use of BL/Source and BL/Sched software products. Without effective management and monitoring of BL/Source and BL/Sched, program files and data may be viewed, executed, or modified by unauthorized users.

BL/Source software is used by MDIT to create, test, approve, and implement source code changes. BL/Sched software is used to schedule routine jobs on the production and development mainframes. BL/Source and BL/Sched are used by DCO primarily to establish new user accounts and monitor user activity; by Agency Services to modify user privileges, update source code, and schedule jobs; and by some State departments to schedule jobs and monitor user activity. The overall administration and management of BL/Source and BL/Sched is controlled by DCO.

We reviewed BL/Source and BL/Sched user access controls for DCO, Agency Services, and 2 of the 5 departments with systems on the mainframes. Our review disclosed:

a. MDIT did not effectively manage user accounts of users with access to BL/Source and BL/Sched. DCO and Agency Services share responsibility for establishing user and file security settings. We noted:

   (1) DCO did not restrict the ability to modify users' access rights in BL/Source to only the appropriate individuals. We noted that 49 (80%) of 61 users at the 2 departments had the ability to modify their access rights and grant themselves or others inappropriate and unauthorized access rights. The ability to modify access rights should belong to a limited number of users with responsibility for BL/Source security.

(2) DCO and Agency Services did not require and maintain approved user access request forms for all BL/Source and BL/Sched users. DCO did not maintain approved user access request forms for any of the four users with administrative access rights. In addition, one Agency Services group did not require or maintain any access request forms. Approved access request forms help to ensure that management has approved each user's access and that users have appropriate access to BL/Source and BL/Sched software.

(3) DCO and Agency Services did not consistently review user lists to ensure that users still required access to BL/Source and BL/Sched. We noted:

(a) DCO informed us that it has completed semiannual reviews of user lists; however, DCO did not document the reviews.

(b) One of the 2 Agency Services groups did not review the user list.

Regular reviews of user accounts and related privileges help to ensure that only authorized users are accessing and using BL/Source and BL/Sched software.

(4) DCO did not have a process to disable user accounts of employees who no longer required access. We noted that DCO did not remove access for 22 (14%) of 153 users and 14 (17%) of 81 users of BL/Sched and BL/Source, respectively. Disabling user access upon employee job change or departure helps prevent unauthorized changes to the production job schedule and program source code.

COBIT states that there should be a set of user account management procedures for establishing, issuing, suspending, modifying, and closing user accounts and related privileges. These procedures should apply to all users, including administrators and internal and external users. Procedures should also include maintaining a formal record, including access levels of all persons registered to use the software, along with a timely and regular review of user accounts and access rights.

b. DCO did not assign to an independent individual, without system administrator access rights, the responsibility for monitoring high-risk user activity. BL/Source and BL/Sched provide reports for monitoring high-risk user activity such as changes to production source code and to mainframe job schedules. DCO reviews the monitoring reports and Agency Services can request monitoring reports for the departments to which it provides services. DCO staff review monitoring reports of high-risk user activity; however, these staff also have administrator access to BL/Source and BL/Sched and, therefore, are not providing an independent review. Also, although some Agency Services groups request monitoring reports to review high-risk user activity, not all Agency Services groups request the reports. Establishing independent reviews of high-risk user activity helps to provide management with assurance that high-risk user activity is appropriate. COBIT states that there should be a division of roles and responsibilities to reduce the possibility that a single individual can bypass a critical control.

c. MDIT did not require users to use strong password compositions. We noted that users' BL/Source and BL/Sched passwords were not required to be a strong minimum password length and were not required to contain a combination of alphanumeric and upper and lower case characters. DMB Administrative Guide procedure 1410.17 states that passwords should be a minimum of 6 to 8 characters and contain a combination of alphanumeric characters. Without effective password controls, MDIT cannot ensure the security and integrity of its mainframe data.

d. MDIT did not develop complete policies and procedures related to user accounts. Specifically, DCO did not create centralized policies and procedures regarding user account management such as assigning, modifying, or revoking user access of BL/Source and BL/Sched users. In addition, Agency Services did not create department specific policies and procedures for assigning the appropriate access rights based on users' job responsibilities for 1 of the 2 departments reviewed. COBIT recommends a documented set of user account management procedures for establishing, issuing, suspending, modifying, and closing user accounts and related privileges. These procedures should apply to all users, including administrators and internal and external users.

RECOMMENDATION

We recommend that MDIT effectively manage and monitor the use of BL/Source and BL/Sched software products.

AGENCY PRELIMINARY RESPONSE

MDIT agrees and will comply with the recommendation.

With regard to part a., MDIT informed us that it will review policies for restricting the ability to modify user access rights in BL/Source. Also, MDIT informed us that it will review policies for authorizing BL/Source and BL/Sched users including ensuring that all forms requesting access to BL/Source and BL/Sched are filed in a central repository within DCO, that access rights are reviewed yearly to ensure that users have not changed roles, and that users no longer needing access are disabled.

With regard to part b., MDIT informed us that it will work with agency security administrators to review the process of monitoring high-risk user activity on a regular basis. This process will be documented and the reviews will be done on a regular basis by November 2010.

With regard to part c., MDIT informed us that it will discuss this issue with the vendor who supplies the BL products to the State. The State will request that the vendor change its solution to accommodate a strong password composition. MDIT anticipates that this change could be implemented by November 2010.

With regard to part d., MDIT informed us that it will develop a policy to define security as it relates to user security accounts for BL/Source and BL/Sched. This policy will be documented and approved by November 2010.

PHYSICAL AND ENVIRONMENTAL CONTROLS

COMMENT

Audit Objective: To assess the effectiveness of MDIT's efforts in establishing physical and environmental controls over the State's mainframe information systems.

Audit Conclusion: MDIT's efforts in establishing physical and environmental controls over the State's mainframe information systems were moderately effective. Our assessment disclosed one reportable condition regarding physical security (Finding 4).

FINDING

4. Physical Security

MDIT had not established effective access controls to the computer facilities that house the Unisys mainframe computers. Without effective physical security controls, MDIT may be unable to effectively prevent unauthorized persons from accessing the mainframes.

Our review of physical security and environmental controls at two computer facilities that contain the mainframes disclosed:

a. MDIT did not periodically review and update the list of persons authorized to access the computer facilities. As of May 2009, MDIT authorized 563 and 515 individuals to access the mainframe production and backup computer facilities, respectively. These individuals included contractors, vendors, internal auditors, programmers, and computer analysts. We noted that 302 of the 563 individuals did not access the production computer facility during the period of January through June 2009. We did not summarize the individuals with access to the mainframe backup computer facility for the period of January through June 2009 because the data was not available. FISCAM states that access to computer facilities should be limited to personnel that routinely have a legitimate need for access to perform their job duties. MDIT should define and document who is authorized to access the computer facilities and periodically review the lists of persons to ensure that they still need access.

b. MDIT did not revoke access to the computer facilities for individuals who no longer required access. We selected 52 individuals with access to the two computer facilities. We judgmentally selected 38 individuals based on job descriptions and randomly selected 14 other individuals to determine if their access to the computer facilities was appropriate. We noted that 16 (31%) individuals were either no longer employed by the State or their job did not require access to the computer facilities. FISCAM states that management should regularly review the list of persons authorized to have physical access to computer facilities. MDIT should periodically conduct reviews of computer facility access lists and revoke access to individuals when necessary.

RECOMMENDATION

We recommend that MDIT establish effective access controls to the computer facilities that house the Unisys mainframe computers.

AGENCY PRELIMINARY RESPONSE

MDIT agrees and will comply with the recommendation. MDIT informed us that DCO and Telecommunication Services, in concert with Enterprise Security, perform an audit every six months of access to hosting centers and Telecommunication Services switch rooms. Also, MDIT informed us that, by March 2010, DCO will document the policy for granting approval for obtaining access to the Hosting Centers and OES will publish a report of all individuals who have not accessed the Hosting Center in the last twelve months and notify those individuals that their access rights will be terminated within 30 days. Further, MDIT informed us that it will utilize data from the Human Resources Management Network (HRMN) to validate that individuals with access to the hosting centers are still employed by the State and any user who has left the State's employment will have his/her access rights disabled.

BACKUP AND DISASTER RECOVERY CONTROLS

COMMENT

Audit Objective: To assess the effectiveness of MDIT's efforts in establishing appropriate backup and disaster recovery controls over the State's mainframe information systems.

Audit Conclusion: MDIT's efforts in establishing appropriate backup and disaster recovery controls over the State's mainframe information systems were moderately effective. Our assessment disclosed one reportable condition regarding backup and disaster recovery processes (Finding 5).

FINDING

5. Backup and Disaster Recovery Processes

MDIT had not established sufficient backup and disaster recovery processes. As a result, MDIT cannot fully ensure that the Unisys mainframe information systems can be restored in a timely manner.

The backup process includes copying data and programs to a separate storage media for the purpose of having multiple copies to prevent the loss of data or programs. Disaster recovery involves defining and documenting plans to help sustain and recover critical information technology resources, information systems, and associated business functions. We noted:

a. MDIT did not periodically test backup files to ensure that its ability to restore the operating system, information systems, and data from backup files in the event of a system failure or disaster. COBIT states that regular testing of the backup files helps to ensure the ability to restore the operating system, applications, and data in the event of disaster.

b. MDIT did not document the testing of its mainframe disaster recovery plan. Documentation of disaster recovery plan testing, including test results, will allow MDIT and participating agencies to improve the existing disaster recovery plan, ensuring that it is designed as efficiently as possible. COBIT states that documentation of test plans should include dates and times of testing, detailed chronology of events, procedures to restore the production environment, and test results.

c. MDIT did not obtain documented MDIT management approval of the mainframe disaster recovery plan. Documented approval of the disaster recovery plan provides assurance that management is aware of, and agrees with, the steps to take to reestablish information technology operations. FISCAM states that key individuals such as senior management should approve the plan.

d. MDIT had not established policies or procedures related to the mainframe backup process. The responsibility for performing mainframe backups is shared between DCO and Agency Services. We noted that DCO and Agency Services lacked backup policies and procedures that specifically addressed frequency of backups, location of backup files, backup file retention, backup file testing, and roles and responsibilities in the process. National Institute of Standards and Technology (NIST) special publication 800-34 states that policies should specify the frequency of backups, location of stored data, file-naming conventions, and backup file rotation frequency.

MDIT informed us that backup frequency and retention schedules are documented within automated backup tools. However, clearly defining backup policies and procedures helps to ensure that management's intentions for backup are clearly communicated, understood, and executed by DCO and Agency Services.

RECOMMENDATION

We recommend that MDIT establish sufficient backup and disaster recovery processes.

AGENCY PRELIMINARY RESPONSE

MDIT agrees with the recommendation and will comply.

With regard to part a., MDIT informed us that, for applications and data, DCO will provide OES with a before and after file recovery test every six months and will work with client agencies to test backups on a yearly basis. For the operating system, MDIT informed us that backups are tested and validated annually via a disaster recovery (DR) test and that operating system files are stored redundantly. MDIT also informed us that application testing of backups will be documented in Strohl for the Unisys mainframe DR Plan at the next yearly test.

With regard to part b., MDIT informed us that it publishes DR dates, times, and details of testing in a variety of sources which are currently available to mainframe users and that system level test results are published to the agencies via a lessons learned document upon completion of testing. Those test results will be published in Strohl after the next test. In addition, MDIT informed us that DCO and OES will work with Agency Services to document joint disaster recovery plans and testing by November 2010.

With regard to part c., MDIT informed us that the DR Plan for the Unisys mainframe is already independently reviewed by OES. DCO will implement a process to specifically have management review and document approval of DR plans by April 2010.

With regard to part d., MDIT informed us that it is developing a policy to define frequency of backups, storage location, tape retention, tape testing, and roles and responsibilities. DCO will meet with agency BL/Pack administrators to review, document, and approve policies and procedures by November 2010.

GLOSSARY

BL/Sched	Software used for automated scheduling of routine jobs on production and development mainframe.
BL/Source	Software used to change source code on production applications.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over information technology.
Data Center Operations (DCO)	A group within MDIT responsible for providing centralized Data Center Hosting services for all State agencies.
department security administrator	A department staff member responsible for coordinating mainframe security within the department.
DMB	Department of Management and Budget.
DR	disaster recovery.
effectiveness	Success in achieving mission and goals.
Federal Information System Controls Audit Manual (FISCAM)	Methodology, issued by the U.S. Government Accountability Office, for performing information system control audits of federal and other governmental entities in accordance with professional standards.
information technology	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.

MDIT	Michigan Department of Information Technology.
National Institute of Standards and Technology (NIST)	An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for information systems used in federal programs.
OES	Office of Enterprise Security.
pack families	One or more physical disks used to store code files, job flow, or any other type of data. Each department using the mainframe is assigned their own pack families.
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 program operations to facilitate decision making by parties responsible for overseeing or initiating corrective action and to improve public accountability.
privileged access	Extensive system access capabilities granted to individuals responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.
reportable condition	A matter that, in the auditor's judgment, 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 objectives of the audit; 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.

Unisys mainframe computer	A large enterprise system designed to meet the computing needs of a large organization.

This Page Left Intentionally Blank

STATE OF MICHIGAN · OFFICE of the AUDITOR GENERAL ·