PERFORMANCE AND FINANCIAL RELATED AUDIT
OF THE

MICHIGAN INFORMATION PROCESSING CENTER

DEPARTMENT OF MANAGEMENT AND BUDGET

December 1998

07-595-97

EXECUTIVE DIGEST

MICHIGAN INFORMATION PROCESSING CENTER

INTRODUCTION

This report, issued in December 1998, contains the results of our performance* and financial related audit* of the Michigan Information Processing Center (MIPC), Department of Management and Budget. The financial related portion of our audit covered the period June 1 through October 31, 1997.

AUDIT PURPOSE

This performance and financial related audit was conducted as part of the constitutional responsibility of the Office of the Auditor General. Performance audits are conducted on a priority basis related to the potential for improving effectiveness* and efficiency*. Financial related audits are conducted at various intervals to permit the Auditor General to express an opinion on the State's financial statements. Also, this audit complements our financial audits of State agencies and the *State of Michigan Comprehensive Annual Financial Report*.

BACKGROUND

MIPC is the State's consolidated data center. MIPC was established by Executive Order 1995-10 for the purpose of centralizing mainframe data processing for the State.

* *See glossary on page 23 for definition.*

MIPC is responsible for providing mainframe computer processing equipment, software, and services for all State agencies.

MIPC supports the two mainframe operating environments, Unisys* and Bull*, used by State agencies. As of June 1996, all State agencies operating on the Unisys system*, with the exception of the Michigan Department of State Police and the Bureau of State Lottery, had "migrated" their applications to MIPC. Agencies operating on the Bull system completed their migration by September 1996.

MIPC had 84 full-time equated positions as of September 30, 1997. MIPC is funded entirely from the Information Technology Revolving Fund* . During fiscal year 1996-97, MIPC had expenditures of approximately $26 million.

AUDIT OBJECTIVE, CONCLUSION, AND NOTEWORTHY ACCOMPLISHMENTS

Audit Objective: To assess the effectiveness of MIPC's general controls* in providing a reliable and secure environment for the operation of the State's information systems.

Conclusion: MIPC's general controls were reasonably effective in providing a reliable and secure environment for the routine operation of the State's information systems. However, we noted one material condition* that would preclude MIPC from providing a reliable and secure environment in the event of a disaster or other critical incident:

- MIPC had not developed and tested a business resumption plan to ensure the continuity of

** See glossary on page 23 for definition.*

information systems processing in the event of an interruption (Finding 1).

We were informed that MIPC did not agree with the judgment that this is a material condition. MIPC stated that, for the first time in the State's history, the State has duplicate mainframe computers, redundant communications, and the necessary technical support to ensure their continued operation. An actual disaster recovery/business resumption plan for the State Lottery was successfully conducted and documented. The MIPC operation, while a work in progress, still provides better disaster recovery/business resumption to State agencies than has existed at any time in history. Further, the central issue is one of the existence of paperwork versus documented capability. The paperwork needs to be developed, but the capability exists; therefore, the material condition judgment is not justified. MIPC expects the documentation to be completed by December 31, 2000.

We also noted five reportable conditions* relating to MIPC's security risk assessments, access controls, monitoring of system activity, system software controls, and policies and procedures (Findings 2 through 6).

Noteworthy Accomplishments: Although MIPC had not performed a comprehensive risk assessment for all aspects of its operations, MIPC's technical support staff did perform a risk assessment of the Unisys operating system environment. The risk assessment identified potential control weaknesses associated with the Unisys

* *See glossary on page 23 for definition.*

production and development systems. This resulted in MIPC developing a corrective action plan to address the identified control weaknesses. During our fieldwork, MIPC completed or started working on most of the items identified in its corrective action plan.

Act 364, P.A. 1996, established a performance objective of having MIPC's services available to its users during 99% of fiscal year 1996-97. For the period that we reviewed (January through July 1997), MIPC had met the availability objective.

AUDIT SCOPE AND METHODOLOGY

Our audit scope was to examine the general controls and other information processing records of the Michigan Information Processing Center. 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 methodology included examining MIPC's information processing and other records for the period March 1994 through October 1997. We made a preliminary assessment of the general controls at MIPC. We then analyzed the information and determined where to concentrate our detailed testing. We designed tests of the general controls and performed those tests to meet our audit objective. We evaluated the results of our testing and reported our findings.

AGENCY RESPONSES

Our report contains 6 findings and 9 corresponding recommendations. The agency preliminary response indicated that MIPC would comply with all 9 of the recommendations; however, it did not agree with the classification of Finding 1 as a material condition.

Ms. Janet E. Phipps, Director
Department of Management and Budget
Lewis Cass Building
Lansing, Michigan

Dear Ms. Phipps:

This is our report on the performance and financial related audit of the Michigan Information Processing Center, Department of Management and Budget. The financial related portion of our audit covered the period June 1 through October 31, 1997.

This report contains our executive digest; description of agency; audit objective, scope, and methodology and agency responses; comment, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

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.

Sincerely,

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

This page left intentionally blank.

TABLE OF CONTENTS

MICHIGAN INFORMATION PROCESSING CENTER
DEPARTMENT OF MANAGEMENT AND BUDGET

INTRODUCTION

COMMENT, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of Agency

Michigan Information Processing Center (MIPC), Department of Management and Budget (DMB), is the State's consolidated data center. MIPC was established by Executive Order 1995-10 for the purpose of centralizing mainframe data processing for the State. MIPC is responsible for providing mainframe computer processing equipment, software, and services for all State agencies. Organizationally, MIPC is part of the DMB Office of Computing and Telecommunications.

MIPC supports two mainframe operating environments, Unisys and Bull, used by State agencies. Effective August 1995, agencies operating on the Unisys system began consolidating operations under MIPC. As of June 1996, all State agencies, except for the Michigan Department of State Police and the Bureau of State Lottery, had "migrated" their applications to MIPC. The Michigan Department of State Police is in the process of migrating its administrative applications to MIPC. The Bureau of State Lottery has contracted with MIPC to provide disaster recovery services. Agencies operating on a Bull system completed their migration by September 1996.

MIPC had 84 full-time equated positions as of September 30, 1997. MIPC is funded entirely from the Information Technology Revolving Fund. During fiscal year 1996-97, MIPC had expenditures of approximately $26 million.

Audit Objective, Scope, and Methodology and Agency Responses

Audit Objective

Our audit objective for the performance and financial related audit of the Michigan Information Processing Center (MIPC), Department of Management and Budget (DMB), was to assess the effectiveness of MIPC's general controls in providing a reliable and secure environment for the operation of the State's information systems.

This audit complements our financial audits of State agencies and the *State of Michigan Comprehensive Annual Financial Report*.

Audit Scope

Our audit scope was to examine the general controls and other information processing records of the Michigan Information Processing Center. 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.

Audit Methodology

Our audit methodology included examining MIPC's information processing and other records for the period March 1994 through October 1997. Our work was performed between June and October 1997. To accomplish our audit objective, our audit methodology included the following phases:

1. Data Gathering Phase

   We collected background information about MIPC. We obtained an understanding of the internal control structure pertaining to: (a) general controls for Unisys and Bull operations, which included information processing, system software, physical security, and management controls, and (b) application controls for the MIPC Unisys Security System.

2. Preliminary Review and Evaluation Phase

   We identified the general controls that are the responsibility of MIPC. We evaluated these controls and made a preliminary assessment of the effectiveness

of the controls. We then used our preliminary assessment to determine the extent of our detailed analysis and testing.

3. Testing Phase

   We examined policies and procedures for the management of MIPC. We analyzed the physical security of MIPC production and development facilities. We interviewed select customer agencies to confirm MIPC's general control responsibilities. In addition, we designed test plans and conducted detailed tests of selected controls. This enabled us to determine the effectiveness of the controls and identify the effects of control weaknesses.

4. Evaluation and Reporting Phase

   We performed a final evaluation of the effectiveness of the general controls in providing a reliable and secure operating environment based on our testing and analysis, and we reported our findings.

Agency Responses

Our report contains 6 findings and 9 corresponding recommendations. The agency preliminary response indicated that MIPC would comply with all 9 of the recommendations; however, it did not agree with the classification of Finding 1 as a material condition.

The agency preliminary response which 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 DMB Administrative Guide procedure 1280.02 require DMB to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENT, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF GENERAL CONTROLS

COMMENT

Background: The control structure for the Michigan Information Processing Center (MIPC), Department of Management and Budget (DMB), consists of general controls over information processing, system software, physical security, and management of information systems. General controls over systems development, program modifications, processing, and file access, as well as application controls, are the responsibility of customer agencies.

General controls apply to all processing carried out within a data processing installation. Although general controls are normally independent of individual computer applications, they provide the framework within which many different applications are processed. Therefore, weaknesses in general controls can adversely affect all applications processed at a data processing installation.

Audit Objective: To assess the effectiveness of MIPC's general controls in providing a reliable and secure environment for the operation of the State's information systems.

Conclusion: MIPC's general controls were reasonably effective in providing a reliable and secure environment for the routine operation of the State's information systems. However, we noted one material condition that would preclude MIPC from providing a reliable and secure environment in the event of a disaster or other critical incident. MIPC had not developed and tested a business resumption plan to ensure the continuity of information systems processing in the event of an interruption. We also noted five reportable conditions relating to MIPC's security risk assessments, access controls, monitoring of system activity, system software controls, and policies and procedures.

Noteworthy Accomplishments: Although MIPC had not performed a comprehensive risk assessment for all aspects of its operations, MIPC's technical support staff did

perform a risk assessment of the Unisys operating system environment. The risk assessment identified potential control weaknesses associated with the Unisys production and development systems. This resulted in MIPC developing a corrective action plan to address the identified control weaknesses. During our fieldwork, MIPC completed or started working on most of the items identified in its corrective action plan.

Act 364, P.A. 1996, established a performance objective of having MIPC's services available to its users during 99% of fiscal year 1996-97. For the period that we reviewed (January through July 1997), MIPC had met the availability objective.

FINDING

1. Business Resumption Plan

MIPC had not developed and tested a business resumption plan to ensure the continuity of information systems processing in the event of an interruption.

Business resumption plans should include controls to ensure the continuity of service across a range of potential disruptions. A comprehensive plan should include coverage for relatively minor interruptions, such as temporary power failures, as well as major disasters, such as fires, natural disasters, or sabotage, that would require re-establishing operations at a remote location. These potential disasters would be identified in a comprehensive risk assessment.

A business resumption plan should also contain an updated and detailed description of all strategies, standards, procedures, schedules, and resources required to complete the recovery process. In addition, a plan should be reviewed and tested periodically to ensure that it will function as intended in the event of a disaster.

MIPC provides information processing resources critical to the operation of 12 agencies. Without a tested business resumption plan, a service interruption at MIPC would significantly impair the State's operations. Statistics noted in one of MIPC's informational presentations, Understanding the Business Resumption Plan, show that data processing facilities with no recovery plan have only a 10% chance of restoring the primary site to its original condition. Facilities with a plan that is maintained and periodically tested have a 98% chance to recover.

RECOMMENDATION

We recommend that MIPC develop and test a business resumption plan to ensure the continuity of information systems processing in the event of an interruption.

AGENCY PRELIMINARY RESPONSE

We were informed that MIPC did not agree with the judgment that this is a material condition. MIPC stated that, for the first time in the State's history, the State has duplicate mainframe computers, redundant communications, and the necessary technical support to ensure their continued operation. An actual disaster recovery/business resumption plan for the State Lottery was successfully conducted and documented. The MIPC operation, while a work in progress, still provides better disaster recovery/business resumption to State agencies than has existed at any time in history. Further, the central issue is one of the existence of paperwork versus documented capability. The paperwork needs to be developed, but the capability exists; therefore, the material condition judgment is not justified. MIPC expects the documentation to be completed by December 31, 2000.

FINDING

2. Security Risk Assessments

MIPC had not performed comprehensive security risk assessments for all aspects of its operations. Also, security risk assessments were not performed periodically or when computer systems, facilities, or other conditions changed.

Risk management is the process of establishing and maintaining information technology security within an organization. Security risk assessments are the means by which risks to computer systems and facilities are identified and analyzed to justify the costs of security safeguards. The objective of security risk assessments is to ensure that the security of a computer system and facilities is cost effective, up-to-date, and responsive to threats against the system. The federal government has acknowledged the important role that risk management plays in the administration of the State's Medicaid program. The State is required to establish and maintain a program for conducting periodic risk assessments of the State Medicaid Management Information System.

The State consolidated 10 data centers into one to form MIPC. As a part of the consolidation process, MIPC contracted with two vendors to provide it with recommendations and plans for proceeding with the consolidations. These documents provided a structured approach for the consolidation and contained recommendations on certain security features that should be instituted at the consolidated data center. However, these plans have not been fully implemented and did not address overall security risk once the consolidated data center began operations.

The consolidation of State data centers provides an opportunity for a more cost-effective security program. However, without periodic comprehensive security risk assessments, security risks at MIPC's production facility may go undetected and uncorrected.

RECOMMENDATIONS

We recommend that MIPC conduct a comprehensive security risk assessment for all aspects of its operations.

We also recommend that MIPC perform security risk assessments periodically and when systems, facilities, or other conditions change.

AGENCY PRELIMINARY RESPONSE

We were informed by MIPC that it will continue to conduct risk assessments on all production systems to include the Unisys A-Series and 2200 mainframes, the Bull 9000 mainframe, the NCR 5100 Data Warehouse, and the Tandem Data Exchange Gateway. We were also informed by MIPC that risk assessments will include a review of the facilities' physical security and the access control and system security of each of the platforms listed above. Completion is scheduled by June 30, 1999.

FINDING

3. Access Controls

MIPC had not established effective control procedures for access to its computer room facilities:

a. MIPC issued electronic cardkeys* to individuals whose primary duties did not require their movement into and out of the computer systems area. Our review identified access cards issued to secretarial, database, vendor support, Department of Treasury, and other non-MIPC staff (custodial and DMB couriers).

   MIPC Information Standards and Procedures (Section 01.OPS.019, Computer Room Access and Security) state that all access to the computer systems area will be controlled by the use of electronic cardkey devices. The electronic cardkeys will be authorized only for individuals whose primary duties require their movement into and out of the computer systems area. Others may gain access by obtaining approval from MIPC's management. They are also required to sign the visitors' log and must be escorted by a data center representative while in the computer systems area.

b. MIPC did not perform timely reviews of the computer rooms' access list. We identified individuals on the list who were no longer employed by vendor support teams but whose computer room cardkey access had not been revoked. In addition, we noted individuals on the list who could not be identified as members of the vendor support teams by MIPC's operations management.

   Timely reviews of the computer rooms' access list would help ensure the appropriateness of individuals granted access to the computer rooms.

c. MIPC did not limit individuals' access to specific computer facilities or limit their working hours to those needed to perform their job responsibilities. Our review identified the Bull system's vendor support staff who required access to

* *See glossary on page 23 for definition.*

only the production computer facility; however, their cardkey allowed access to the development computer facility. Our review also disclosed individuals whose cardkeys did not limit their access to MIPC to their normal working hours.

The cardkey access system allows MIPC to limit an individual's access to the required facility, time-of-day, and door necessary to complete job responsibilities.

d. MIPC Information Standards and Procedures (Section 01.OPS.019, Computer Room Access and Security) identify the MIPC operations manager as the responsible party for controlling computer room access. We determined that MIPC had not developed procedures for authorizing the assignment of electronic cardkeys used to access the computer rooms.

e. MIPC did not secure access to the computer room and print room within the development computer facility. These rooms at the development computer facility did not contain locking devices. Although access to the development computer facility is controlled with magnetic card access devices, the facility is shared with non-MIPC operations staff. As such, individuals who are not a part of MIPC operations could access the computer room and print room.

Ineffective access controls increase the risk of inappropriate use of computer room facilities.

RECOMMENDATION

We recommend that MIPC establish effective control procedures for access to its computer room facilities.

AGENCY PRELIMINARY RESPONSE

MIPC agreed with this recommendation and will comply by March 31, 1999. MIPC informed us that it and the Office of Computing and Telecommunications security personnel have already taken steps to ensure that only those personnel who are authorized are granted access to the data center and only at the appropriate times. MIPC also informed us that a further security review aimed at enhancing the

access controls is under way and the results will be used to strengthen the security of all aspects of the data center operation.

FINDING

4. Monitoring of System Activity

MIPC had not established control procedures to monitor system activity as required by MIPC and State standards:

a. MIPC did not ensure that computer system logs* provided sufficient audit trails of activities performed on the Bull system. The computer system logs did not indicate which files were accessed and by whom the files were accessed.

A third party assessment of Bull system controls identified the need to protect critical system, database, program, and job control language files. For example, system logs must provide an adequate audit trail of who accessed system files and used privileged* programs and commands. The assessment recommended how this could be accomplished; however, MIPC did not implement the recommendation.

To provide accountability for activity occurring on a computer system, automated system logs should identify the files accessed and by whom. Without a complete audit trail, unauthorized changes could occur to critical files and MIPC would be unable to hold a specific individual accountable.

b. MIPC did not monitor computer console activities. This condition existed on both the Unisys and Bull systems.

Computer operators and technical support staff enter commands at a console to manage and control a system's activity and resources. Some of the actions performed at the computer console may be considered security risks. DMB Administrative Guide procedure 1310.02 requires data centers to establish and implement procedures for monitoring computer console activities to identify security and procedural violations.

* *See glossary on page 23 for definition.*

MIPC's Unisys Corrective Action Plan includes developing a report to monitor the use of console commands that it considers security risks; however, MIPC had not implemented the plan at the close of our fieldwork. Also, the Bull data center consolidation contractor recommended that MIPC comply with DMB Administrative Guide procedure 1310.02; however, MIPC had not taken action on the contractor's recommendation.

The lack of monitoring increases the risk that MIPC may not detect unauthorized computer console activity.

c. MIPC did not monitor the activities of its privileged users or the use of privileged programs. This condition existed on both the Unisys and Bull systems.

MIPC Information Standards and Procedures (Section 01.OPS.036, Privileged Usercode Policy) state that daily reports will be produced indicating the activity performed under privileged usercodes. The reports are to be reviewed by the MIPC security administrator.

Ongoing monitoring of privileged users and privileged programs is necessary because privileged users and privileged programs have the ability to bypass system software security. The lack of monitoring increases the risk that MIPC may not detect unauthorized access and changes to files.

RECOMMENDATIONS

a) We recommend that MIPC ensure that computer system logs provide sufficient audit trails of activities performed on the Bull system.

b) We recommend that MIPC monitor computer console activities.

c) We recommend that MIPC monitor the activities of its privileged users and the use of privileged programs.

AGENCY PRELIMINARY RESPONSE

(a) MIPC agreed with this recommendation and will comply by March 31, 1999. MIPC informed us that the computer system logs will be maintained in sufficient detail to provide a means to appropriately control the operation of the Bull system and its operating environment.

(b) MIPC agreed with this recommendation and will comply by March 31, 1999. MIPC informed us that it will establish written procedures to monitor the system activity controlled at the computer consoles. Further, operators will be advised as to the use and intent of the written procedures.

(c) MIPC agreed with this recommendation and will comply by March 31, 1999. MIPC informed us that the Office of Computing and Telecommunications security group, not MIPC, will monitor and control the activity of privileged users and the use of privileged programs.

FINDING

5. System Software Controls

MIPC had not developed control procedures to prevent or detect the processing of unauthorized transactions while using system software utilities. This condition existed for both the Unisys and Bull systems.

MIPC provided several system software utilities to manage customer agencies' files and application programs. Customer agencies used these same utilities to control job scheduling, program changes, and tape file management. At the direction of each customer agency, MIPC enters the customer agency's access capabilities and the agency's requirements for tape file retention.

MIPC may make inadvertent changes that could adversely affect customer agencies. For example, if MIPC accidentally made changes to an agency's tape file retention, this could result in the loss of critical customer agency tape files without the agency becoming aware of it until the next time the tape files were accessed for use.

Effective control procedures would provide a method, where practical, for MIPC to prevent an unauthorized transaction from occurring, as well as methods for customer agencies to detect and correct unauthorized transactions if they do occur.

To establish effective control procedures, the software vendor would need to modify its product or MIPC and customer agencies would need to establish compensating controls.

RECOMMENDATION

We recommend that MIPC develop control procedures to prevent or detect the processing of unauthorized transactions while using system software utilities.

AGENCY PRELIMINARY RESPONSE

MIPC agreed with this recommendation and will comply by March 31, 1999. MIPC informed us that, where practical and necessary, it will institute control procedures to monitor and prevent the inadvertent and/or deliberate processing of unauthorized transactions while using system software utilities.

FINDING

6. Policies and Procedures

MIPC had not developed comprehensive policies and procedures for all functional areas of its operations.

We noted that MIPC had developed policies and procedures covering the operation of the Unisys system. However, we also noted the following areas in which MIPC relied on employee practices, memorandums, letters, and e-mail rather than written policies and procedures:

a. MIPC had not developed written procedures for tracking hardware and software problems and the resolution of the problems.

MIPC used several tracking processes for problems related to the Bull system. However, we determined that MIPC had not documented when operators should use each tracking process.

b. MIPC had not developed written procedures to address tape library functions, such as pulling tapes from the tape library, logging tapes in and out, entering tape retention periods, and reviewing scratch and move tape listings.

DMB Administrative Guide procedure 1310.02 states that procedures must be established for the librarian's function.

c. MIPC had not developed complete written procedures for the Bull system's computer operations.

Written procedures should cover such items as those noted in the operators' loose leaf binder located in the computer operations room. The loose leaf binder contained some procedures, memorandums, and hand-written notes related to the various operation functions performed by the operators. We were informed that other procedures covering miscellaneous operational tasks existed in several forms. The various sources for operational procedures should be standardized and incorporated into an operations manual.

d. MIPC operations did not have written procedures for managing environmental conditions. Environmental conditions must be defined and documented for the computer room. Procedures should include identifying who is responsible for monitoring environmental conditions, how staff should respond to conditions that may arise, and what to do for emergency interruptions in service.

e. MIPC was in the process of developing various personnel-related policies and procedures. However, we identified several additional areas that should be included: supplemental employment and employee conflicts of interest (see Sections 2-15 and 2-21, respectively, of the *Rules of the Civil Service Commission*), employee background security checks, and employee terminations.

f. MIPC had not established procedures for investigating security breaches. A third party review of MIPC security controls noted that an incident recovery plan should include what constitutes a security breach or intrusion, directions for reporting an intrusion, and guidelines for an appropriate response.

g. MIPC had not established procedures to ensure that the Bull operating system is adequately documented. In addition, we determined that MIPC did not maintain a complete audit trail of all modifications to the Bull operating system.

Written procedures are an effective control technique in ensuring that management's directives are carried out as intended. In addition, DMB Administrative Guide procedure 1310.02 requires written procedures for many of the conditions noted above.

RECOMMENDATION

We recommend that MIPC develop policies and procedures for all functional areas of its operations.

AGENCY PRELIMINARY RESPONSE

MIPC agreed with this recommendation and will comply by March 31, 1999. MIPC informed us that it will develop policies and procedures to enhance existing State policy and for areas in which no policy currently exists. MIPC also informed us that a survey of the necessary operational areas will be conducted to establish the priority order for the development of the needed policies and procedures.

Glossary of Acronyms and Terms

Bull	A mainframe computer manufacturer.
computer system log	An audit trail of system activity (e.g., files accessed, jobs processed, and commands entered at the computer console).
DMB	Department of Management and Budget.
effectiveness	Program success in achieving mission and goals.
efficiency	Achieving the most outputs and outcomes practical for the amount of resources applied or minimizing the amount of resources required to attain a certain level of outputs or outcomes.
electronic cardkey	A device used to control access to the computer room area.
financial related audit	An audit that includes determining whether (1) financial information is presented in accordance with established or stated criteria, (2) the entity has adhered to specific financial compliance requirements, or (3) the entity's internal control structure over financial reporting and/or safeguarding assets is suitably designed and implemented to achieve the control objectives.
general controls	General controls apply to all processing carried out within a data center processing installation. Although general controls are normally independent of individual computer applications, they provide the framework within which many different applications are processed. Therefore, weaknesses in general controls can adversely affect all applications processed at the data processing installation.

Information Technology Revolving Fund	This Fund was created, by administrative decision, to provide telecommunication and information technology services for State agencies. Administrative costs are appropriated in the General Fund and financed by interfund transfers. The cost of providing services is charged to user agencies on a monthly basis.
material condition	A serious reportable condition which could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the opinion of an interested person concerning the effectiveness and efficiency of the program.
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.
privileged	Usercodes or programs that have the capability to bypass normal system and file security.
reportable condition	A matter coming to the auditor's attention that, in his/her judgment, should be communicated because it represents either an opportunity for improvement or a significant deficiency in the design or operation of the internal control structure or in management's ability to operate a program in an effective and efficient manner.
system	A system normally includes hardware, software, information, data, applications, communications, and people.
Unisys	A mainframe computer manufacturer.