MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

GENERAL CONTROLS OVER THE DATA COLLECTION AND DISTRIBUTION SYSTEM (DCDS) AND THE HUMAN RESOURCES MANAGEMENT NETWORK (HRMN)

OFFICE OF THE STATE BUDGET,
CIVIL SERVICE COMMISSION, AND
MICHIGAN DEPARTMENT OF INFORMATION TECHNOLOGY

September 2009

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

084-0597-09

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

General Controls Over the Data Collection and Distribution System(DCDS) and the Human Resources Management Network (HRMN)

Office of the State Budget, Civil Service Commission, and Michigan Department of Information Technology

Report Number:
084-0597-09

Released:
September 2009

DCDS and HRMN process the State of Michigan employee payroll. DCDS records, allocates, and distributes payroll costs within the accounting system. HRMN processes personnel, payroll, and employee benefits data. For fiscal year 2007-08, DCDS and HRMN processed approximately $4.9 billion in State employee payroll expenditures.

Audit Objective:
To assess the effectiveness of the Michigan Department of Information Technology's (MDIT's) security and access controls over the DCDS and HRMN operating systems.

Audit Conclusion:
MDIT's security and access controls over the DCDS and HRMN operating systems were not effective. Although MDIT had implemented some measures to reduce the operating systems' exposure to security threats, we identified weaknesses in critical aspects of the operating systems. We noted one material condition (Finding 1).

Material Condition:
MDIT had not fully established security and access controls over the DCDS and HRMN operating systems (Finding 1).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of MDIT's security and access controls over the DCDS and HRMN database management systems.

Audit Conclusion:
MDIT's security and access controls over the DCDS and HRMN database management systems were not effective. Although MDIT had implemented some measures to reduce the database management systems' exposure to security threats, we identified weaknesses in critical aspects of the database management systems. We noted one material condition (Finding 2).

Material Condition:
MDIT had not fully established security and access controls over the DCDS and HRMN databases (Finding 2).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of MDIT's configuration management controls over DCDS and HRMN.

Audit Conclusion:
MDIT's configuration management controls over DCDS and HRMN were moderately effective. We noted one reportable condition (Finding 3).

Reportable Condition:
MDIT had not fully established change control processes to ensure that all DCDS and HRMN operating system and database management system changes were authorized, tested, and implemented with appropriate risk based controls (Finding 3).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 3 findings and 3 corresponding recommendations. The Office of the State Budget, Civil Service Commission, and MDIT's preliminary response indicates that they agree with all of the recommendations and have complied or 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

September 18, 2009

Mr. Robert L. Emerson, State Budget Director
Office of the State Budget
Department of Management and Budget
George W. Romney Building
Lansing, Michigan
and
Mr. Jeremy S. Stephens, State Personnel Director
Civil Service Commission
Capitol Commons Center
Lansing, Michigan
and
Mr. Kenneth D. Theis, Director
Michigan Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Mr. Emerson, Mr. Stephens, and Mr. Theis:

This is our report on the performance audit of General Controls Over the Data Collection and Distribution System (DCDS) and the Human Resources Management Network (HRMN), Office of the State Budget, Civil Service Commission, and Michigan Department of Information Technology.

This report contains our report summary; description of agencies and systems; 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 agencies' response subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agencies 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

GENERAL CONTROLS OVER THE DATA COLLECTION AND DISTRIBUTION SYSTEM (DCDS) AND THE HUMAN RESOURCES MANAGEMENT NETWORK (HRMN) OFFICE OF THE STATE BUDGET, CIVIL SERVICE COMMISSION, AND MICHIGAN DEPARTMENT OF INFORMATION TECHNOLOGY

Description of Agencies and Systems

The Data Collection and Distribution System (DCDS) and the Human Resources Management Network (HRMN) process the State of Michigan employee payroll. DCDS records, allocates, and distributes payroll costs within the accounting system. HRMN processes personnel, payroll, and employee benefits data. For fiscal year 2007-08, DCDS and HRMN processed approximately $4.9 billion in State employee payroll expenditures.

Office of the State Budget, Department of Management and Budget

The Office of Financial Management's (OFM's) Payroll and Tax Reporting Division is responsible for the operation of HRMN, payroll tax reporting, W-2 reporting, backup withholding, and 1099 reporting. In carrying out these responsibilities, the Payroll and Tax Reporting Division takes a leadership role in defining Statewide policies regarding payroll and tax reporting. In addition, OFM's Support Services Division is responsible for operating DCDS and HRMN help desks. The Support Services Division also processes DCDS security* requests and develops security related policies and procedures.

Civil Service Commission (CSC), Department of Management and Budget

Executive Order No. 2002-19 established the executive direction and management of HRMN in the Department of Civil Service. Executive Order No. 2007-30 transferred all responsibilities of the Department of Civil Service to CSC. In addition, the Executive Order established CSC as an autonomous agency under the Department of Management and Budget. Among other things, CSC's Business Applications Support Section is responsible for HRMN application security.

Michigan Department of Information Technology (MDIT)

MDIT's Technical Services Division is responsible for maintaining and supporting the DCDS and HRMN operating systems. In addition, MDIT's Bureau of Agency Services provides technical support for DCDS and HRMN application development and maintenance, database management, and help desk services.

* *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 General Controls* Over the Data Collection and Distribution System (DCDS) and the Human Resources Management Network (HRMN), Office of the State Budget (OSB), Civil Service Commission (CSC), and Michigan Department of Information Technology (MDIT), had the following objectives:

1. To assess the effectiveness* of MDIT's security and access controls* over the DCDS and HRMN operating systems*.

2. To assess the effectiveness of MDIT's security and access controls over the DCDS and HRMN database management systems*.

3. To assess the effectiveness of MDIT's configuration management* controls over DCDS and HRMN.

Audit Scope

Our audit scope was to examine the information processing and other records related to selected Data Collection and Distribution System and Human Resources Management Network general controls. 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 June through August 2008 and from February through May 2009, generally covered the period October 2007 through May 2009.

Audit Methodology

The criteria used in the audit included control techniques and suggested audit procedures from the U.S. Government Accountability Office's (GAO's) *Federal Information System Controls Audit Manual,* control objectives and audit guidelines outlined in the Control Objectives for Information and Related Technology* (COBIT) issued by the IT

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

Governance Institute, and other 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 of general controls over DCDS and HRMN. We obtained an understanding of DCDS and HRMN system architectures. We identified and reviewed best practices for operating system and database management system security. This included guidance from the Center for Internet Security, the SANS Institute, the Internal Revenue Service, and software vendors. We used the results of our preliminary review to determine the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase

   We performed an assessment of select general controls over the DCDS and HRMN operating systems and database management systems. Specifically, we assessed:

   a. Operating System Security and Access:

      We interviewed DCDS and HRMN system administrators* and other MDIT staff to obtain an understanding of MDIT's strategy to secure the DCDS and HRMN operating systems. We reviewed and tested operating system configurations for DCDS and HRMN. We assessed the appropriateness of users' access to the DCDS and HRMN operating systems.

   b. Database Management System Security and Access:

      We interviewed DCDS and HRMN database administrators* to gain an understanding of access controls within the DCDS and HRMN databases. We reviewed and tested database management system configurations for DCDS and HRMN. We assessed the appropriateness of users' access to the DCDS and HRMN database management systems.

   c. Configuration Management:

      We interviewed MDIT management to obtain an understanding of the Local Change Control Board and the Enterprise Change Control Board processes.

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

We reviewed and assessed MDIT policies and procedures for requesting, evaluating, implementing, and tracking changes to operating system and database management system configurations, including emergency changes. We tested a selection of configuration changes to the DCDS and HRMN operating systems and database management systems and determined whether the changes had been properly approved, tested, and documented.

Our audit was not directed toward examining changes to the DCDS and HRMN application code and data. Therefore, we did not conclude on the appropriateness of these changes.

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 Responses and Prior Audit Follow-Up

Our audit report contains 3 findings and 3 corresponding recommendations. OSB, CSC, and MDIT's preliminary response indicates that they agree with all of the recommendations and have complied or will comply with them.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' 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 OSB, CSC, and MDIT to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

We released our prior performance audit of the Data Collection and Distribution System, Michigan Administrative Information Network, Department of Management and Budget (07-599-00), in August 2001. Within the scope of this audit, we followed up 1 of the 5 prior audit recommendations. The prior audit recommendation was rewritten for inclusion in this report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

OPERATING SYSTEM SECURITY AND ACCESS

COMMENT

Background: Access controls limit or detect inappropriate access to computer resources, such as an information system's operating system. In its October 2008 bulletin, the Information Technology Laboratory, National Institute of Standards and Technology* (NIST), explained that the first step in ensuring the security of an information system is securing its operating system. Securing the operating system is necessary because operating system manufacturers, who are unaware of each organization's unique security requirements, often configure their hardware and software to emphasize functionality and ease of use at the expense of security.

Audit Objective: To assess the effectiveness of the Michigan Department of Information Technology's (MDIT's) security and access controls over the Data Collection and Distribution System (DCDS) and Human Resources Management Network (HRMN) operating systems.

Audit Conclusion: MDIT's security and access controls over the DCDS and HRMN operating systems were not effective. Although MDIT had implemented some measures to reduce the operating systems' exposure to security threats*, we identified weaknesses in critical aspects of the operating systems. Our assessment disclosed one material condition*. MDIT had not fully established security and access controls over the DCDS and HRMN operating systems (Finding 1).

FINDING

1. Operating System Security and Access Controls

MDIT had not fully established security and access controls over the DCDS and HRMN operating systems. As a result, individuals may circumvent or modify DCDS and HRMN application controls designed to ensure the accuracy and completeness of payroll transactions and the integrity* of payroll data.

According to NIST, controls to protect operating systems generally fall into two major categories: eliminating or mitigating known security vulnerabilities and granting access based on the principle of least privilege*. Using industry best

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

practices and vendor recommendations, we reviewed the DCDS and HRMN operating system configurations. Our review disclosed:

a. MDIT had not configured DCDS and HRMN to enforce strong password and account lock-out policies.

b. MDIT did not restrict access to the operating systems' privileged account*. We identified contractors and users besides the system administrator with knowledge of the privileged account's password.

c. MDIT did not fully prohibit remote log-ins with the operating systems' privileged account.

d. MDIT had not removed or disabled unnecessary start-up scripts and services with known vulnerabilities*. For some services, MDIT indicated that there may be a legitimate business purpose for the service. However, MDIT had not fully investigated more secure alternatives or implemented compensating controls.

e. MDIT had not fully implemented operating system security features and did not ensure that all security related parameters were properly configured.

f. MDIT had not secured all sensitive operating system, application, and data files.

g. MDIT did not routinely monitor system administrator and other privileged activity.

h. MDIT had not established procedures to ensure that security events were routinely monitored and to ensure that monitoring activities were documented. Although the system administrator informed us that he monitored log files for security events, MDIT was unable to provide documentation to support the types of security events monitored, the frequency of review, and actions taken.

MDIT used firewalls* to reduce the operating systems' exposure from external hackers*. However, it is equally important for MDIT to ensure that its operating systems are properly secured from insider threats. For example, the 2007 E-Crime

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

Watch Survey (conducted by the U.S. Secret Service, the CERT(R) Coordination Center (CERT/CC), Microsoft, and *CSO* magazine) disclosed that insiders have significant advantages over external hackers because they can often bypass physical and logical security measures directed at defending against external hackers. In addition, insiders are often aware of loosely enforced policies and procedures and exploitable control weaknesses in networks and information systems.

The security and access weaknesses we identified can be attributed to weaknesses in the application design of HRMN and to the fact that MDIT had not ensured that the system administrators fully implemented MDIT's server security policy. MDIT policy 1350.11 requires the development of a server plan that includes, among other things, risk assessments*, minimum server hardening, host based intrusion detection, and audit and monitoring.

RECOMMENDATION

We recommend that MDIT fully establish security and access controls over the DCDS and HRMN operating systems.

AGENCY PRELIMINARY RESPONSE

MDIT agrees with the recommendation to establish more effective operating system security and access controls. MDIT informed us that it has remediated the security and access control weaknesses identified in part b. and part c.. In addition, MDIT informed us that it will implement appropriate controls depending upon cost assessments, potential benefits, levels of risk, and impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.

DATABASE MANAGEMENT SYSTEM SECURITY AND ACCESS

COMMENT

Background: In addition to securing an information system's operating system, it is equally important to protect the data stored in the database management system.

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

Modern database management systems have many features and capabilities that can be used to compromise the availability*, confidentiality*, and integrity of data. Unless properly secured, poor database management system security not only compromises the database but may also compromise the information system's operating system and other trusted network systems.

Audit Objective: To assess the effectiveness of MDIT's security and access controls over the DCDS and HRMN database management systems.

Audit Conclusion: MDIT's security and access controls over the DCDS and HRMN database management systems were not effective. Although MDIT had implemented some measures to reduce the database management systems' exposure to security threats, we identified weaknesses in critical aspects of the database management systems. Our assessment disclosed one material condition. MDIT had not fully established security and access controls over the DCDS and HRMN databases (Finding 2).

FINDING

2. Database Security and Access Controls

MDIT had not fully established security and access controls over the DCDS and HRMN databases. Fully establishing database security and access controls would help prevent or detect inappropriate access and modification to DCDS and HRMN data.

According to ISO/IEC 27002:2005*, *Information technology - Security techniques - Code of Practice for Information Security Management,* a well-secured database provides a protected environment to maintain the integrity and confidentiality of data. Appropriate security controls include using individual user accounts and passwords, monitoring user activities to ensure that users are performing only the activities that they are explicitly authorized to perform, and using audit logs to record and monitor significant events. Our review of the DCDS and HRMN databases disclosed:

a. MDIT had not fully developed and implemented policies and procedures for managing database security and access. For example, MDIT had not established policies and procedures for granting privileged or other direct

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

database access, hardening the database management system, maintaining a secure database configuration, and monitoring privileged activities. Without complete policies and procedures, security controls may be inadequate and responsibilities may not be assigned and properly fulfilled so that controls may be consistently applied.

b. MDIT had not established unique user accounts for the DCDS and HRMN database administrators (DBAs). In addition, DCDS's DBAs used the DCDS application account to perform their DBA responsibilities. Shared accounts negate management's ability to assign responsibility and to effectively monitor DBA activity.

c. MDIT did not effectively monitor the activity of DCDS and HRMN's DBAs and other privileged accounts. Although MDIT did monitor the personal account of DCDS's primary DBA, the DBA did not use this account to perform privileged activities. Because privileged accounts have the ability to bypass established controls, all privileged account activity should be logged and monitored.

d. MDIT had not developed a strategy to detect and monitor security violations and unauthorized database activity. The database management system has audit logs that can be configured to record sensitive database activity. However, without a strategy to log and monitor unusual database activity, MDIT cannot be assured that security violations would be detected.

e. MDIT did not effectively configure security settings such as password settings, profile settings, and configuration parameters for the DCDS and HRMN databases. Properly configured database security settings help to prevent unauthorized access and ensure the integrity of data within the DCDS and HRMN databases.

f. MDIT had not removed excessive access that the database management system granted by default to all database accounts. As such, DCDS and HRMN users have access to database resources beyond their business need, which could be exploited to gain unauthorized access.

We reported similar control weaknesses in our performance audit of DCDS, released in August 2001. The Department of Management and Budget (DMB) agreed with the recommendation and indicated that it would comply by

September 30, 2001. However, DMB had not resolved the control weaknesses by October 2001, when MDIT assumed primary responsibility for DCDS and HRMN general controls.

RECOMMENDATION

We recommend that MDIT fully establish security and access controls over the DCDS and HRMN databases.

AGENCY PRELIMINARY RESPONSE

MDIT agrees with the recommendation regarding improvements to DCDS and HRMN database security and access controls. MDIT informed us that, in conjunction with the Office of Financial Management (OFM) and the Civil Service Commission (CSC), it will evaluate and remediate the security and access controls over the DCDS and HRMN databases depending upon the potential risks involved, the potential solutions, and the availability of State resources.

CONFIGURATION MANAGEMENT CONTROLS

COMMENT

Background: Configuration management controls provide reasonable assurance that all changes to information system resources are authorized and that systems are configured and operated securely and as intended.

In December 2007, MDIT established the Enterprise Change Governance Board (ECGB), whose goal is to ensure that standardized methods and procedures are used for efficient and prompt handling of all information technology* (IT) changes. ECGB's governance model for IT changes is based on the Information Technology Infrastructure Library (ITIL). Before the creation of MDIT, OFM and CSC were responsible for changes to the DCDS and HRMN operating and database management systems.

Audit Objective: To assess the effectiveness of MDIT's configuration management controls over DCDS and HRMN.

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

Audit Conclusion: MDIT's configuration management controls over DCDS and HRMN were moderately effective. Our assessment disclosed one reportable condition* related to DCDS and HRMN change controls (Finding 3).

FINDING

3. DCDS and HRMN Change Controls

MDIT had not fully established change control processes to ensure that all DCDS and HRMN operating system and database management system changes were authorized, tested, and implemented with appropriate risk based controls. Without proper controls, there is a risk that inadvertent or intentional changes to the operating and database management systems may adversely impact the proper functioning of the State's payroll applications or the integrity of the State's payroll data.

Control Objectives for Information and Related Technology (COBIT) states that all changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment should be formally managed in a controlled manner.

Our review of MDIT's change control practices and our examination of selected operating system and database management system changes disclosed:

a. MDIT had not fully developed and implemented formal enterprise change control policies and procedures. COBIT states that formal change control policies and procedures should be established to ensure that all changes are handled in a standardized manner. MDIT's ECGB had several draft policies and other informal documentation. However, the policies and documentation had not been formally adopted by management and did not reflect a comprehensive change control process. For example, MDIT had not established change control policies and procedures for defining roles and responsibilities, categorizing changes, assessing security impact and risk, segregating incompatible responsibilities, and monitoring for unauthorized changes. OFM, CSC, and MDIT's Bureau of Agency Services provided us with documented change control procedures; however, the procedures focused primarily on application changes rather than overall operating system and database management system changes.

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

b. MDIT's enterprise change control process did not categorize changes by type (i.e., application, operating system, or database management system) and significance (i.e., high impact, medium impact, or low impact). ITIL recommends that changes be categorized by type and by significance so that standard change control processes can be developed based on the level of risk.

c. MDIT did not assess the security impact and did not sufficiently describe the potential risks associated with each change. An insufficient assessment and description of the security impact and risks may impair management's ability to make informed decisions about the appropriate level of testing and the approvals required for each change.

d. MDIT, in conjunction with OFM and CSC, did not routinely perform integrated testing* of operating system changes before implementing them in the production environment. OFM informed us that in 2006 it began performing integrated testing for database management system changes after an untested change adversely impacted the application. Because untested operating system changes pose similar risks to payroll data and processing as untested database management system changes, MDIT should perform integrated testing of operating system changes.

e. MDIT had not established controls to monitor the effectiveness of its change control processes. For example, MDIT had not fully established a baseline configuration for the DCDS and HRMN operating and database management systems and a means to automatically detect changes made to the baseline configuration. ITIL recommends that, at least annually, management, independent of those making the changes, review changes for compliance with established policies and procedures. An effective monitoring process would help MDIT ensure that any unauthorized operating system or database management system changes are detected.

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

RECOMMENDATION

We recommend that MDIT fully establish change control processes to ensure that all DCDS and HRMN operating system and database management system changes are authorized, tested, and implemented with appropriate risk based controls.

AGENCY PRELIMINARY RESPONSE

MDIT agrees with the recommendation to enhance the procedures and documentation that exist within the DCDS and HRMN change control process. MDIT informed us that, in conjunction with OFM and CSC, it is already working to implement solutions for some aspects of the recommendation. In addition, MDIT, OFM, and CSC informed us that they will continue to identify additional improvements to this process, assess the impact of potential solutions, and prioritize and implement changes based on the potential risks and availability of State resources.

GLOSSARY

Glossary of Acronyms and Terms

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
availability	Timely and reliable access to data and information systems.
confidentiality	Protection of data from unauthorized disclosure.
configuration management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.
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.
CSC	Civil Service Commission.
database administrator (DBA)	The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users of the database. Additional responsibilities include operation, performance, integrity, and security of the database.
database management system	A software product that aids in controlling and using the data needed by application programs. Database management systems organize data in a database; manage all requests for database actions, such as queries or updates from users; and permit centralized control of security and data integrity.
DCDS	Data Collection and Distribution System.
DMB	Department of Management and Budget.

ECGB	Enterprise Change Governance Board.
effectiveness	Program success in achieving mission and goals.
firewall	Hardware and software components that protect one set of system resources (e.g., computers or networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.
general controls	The structure, policies, and procedures that apply to an entity's overall computer operations. These controls include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.
hacker	A person who attempts to enter a system without authorization from a remote location.
HRMN	Human Resources Management Network.
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.
integrated testing	Testing that focuses on interfaces between and among components of the application, such as functional correctness, system stability, overall system operability, system security, privacy and sensitive information control, and system performance requirements.
integrity	Accuracy, completeness, and timeliness of data in an information system.

ISO/IEC 27002:2005	A security standard published by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in the standard provide general guidance on the commonly accepted goals of information security management.
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.
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 federal programs.
OFM	Office of Financial Management.
operating system	The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running.
OSB	Office of the State Budget.
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.
principle of least privilege	A basic principle in information security that holds that entities (people, processes, and devices) should be assigned the fewest privileges consistent with their assigned duties and functions.
privileged account	The account that has access to all commands and files on a operating system or database management system.
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.
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. Risk assessment is a part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
security	Safeguarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
system administrator	The person responsible for administering use of a multiuser computer system, communications system, or both.

threat	Any circumstance or event with the potential to adversely impact entity operations (including mission, functions, image, or reputation), entity assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL