MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

SELECTED GENERAL AND APPLICATION CONTROLS

DEPARTMENT OF ENVIRONMENTAL QUALITY AND
DEPARTMENT OF INFORMATION TECHNOLOGY

December 2006

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

761-0590-05

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

Selected General and Application Controls

Department of Environmental Quality and Department of Information Technology

Report Number:
761-0590-05

Released:
December 2006

The Department of Environmental Quality (DEQ) maintains and operates 136 information systems to accomplish its mission. The Department of Information Technology (DIT) provides information support services to DEQ, including operating system configuration, application development and maintenance, database administration, program and data change controls, and backup and recovery controls.

Audit Objective:
To assess the effectiveness of DEQ and DIT's efforts in establishing appropriate security and access controls over data and data systems.

Audit Conclusion:
DEQ and DIT were not effective in their efforts to establish appropriate security and access controls over data and data systems.

Material Condition:
DEQ, in conjunction with DIT, had not established and implemented an information systems security program and security and access controls over data and data systems (Finding 1).

Reportable Condition:
DIT had not established effective security and access controls over the server operating systems (Finding 2).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DEQ and DIT's efforts in establishing appropriate change management controls over data and data systems.

Audit Conclusion:
DEQ and DIT were not effective in their efforts to establish appropriate change management controls over data and data systems.

Material Condition:
DEQ and DIT had not established effective change management controls (Finding 3).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DEQ and DIT's efforts in establishing appropriate backup and recovery controls over data and data systems.

Audit Conclusion:
DEQ and DIT were not effective in their efforts to establish appropriate backup and recovery controls over data and data systems.

Reportable Condition:
DEQ and DIT had not evaluated the criticality of DEQ's data and data systems to implement effective backup and recovery controls (Finding 4).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DEQ and DIT's efforts to ensure the integrity of data for Navision and LABWORKS.

Audit Conclusion:
DEQ and DIT were moderately effective in their efforts to ensure the integrity of data for Navision and LABWORKS.

Reportable Condition:
DEQ did not fully ensure the integrity of data for Navision and LABWORKS (Finding 5).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 5 findings and 5 corresponding recommendations. DEQ's and DIT's preliminary responses indicate that they agree 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

December 22, 2006

Mr. Steven E. Chester, Director
Department of Environmental Quality
Constitution Hall
Lansing, Michigan
and
Ms. Teresa M. Takai, Director
Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Mr. Chester and Ms. Takai:

This is our report on the performance audit of Selected General and Application Controls, Department of Environmental Quality and Department of Information Technology.

This report contains our report summary; description of agencies; 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 agencies' responses 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

SELECTED GENERAL AND APPLICATION CONTROLS
DEPARTMENT OF ENVIRONMENTAL QUALITY AND
DEPARTMENT OF INFORMATION TECHNOLOGY

Department of Environmental Quality (DEQ)

DEQ information systems contain environmental data necessary to protect public health and preserve the State's environmental resources. DEQ maintains and operates 136 information systems to accomplish its mission. DEQ maintains and operates the following information systems to record and process essential financial and environmental data:

a. Navision

Navision is DEQ's centralized information management system for cash receipting and invoicing.

DEQ's Office of Financial Management (OFM) enters cash receipts into Navision at the Lansing central office. DEQ enters invoices into Navision at the Lansing central office, at DEQ district offices, and from DEQ's other information systems using the AAToolkit interface. The AAToolkit interface was developed by the Department of Information Technology (DIT) to import data from DEQ's other information systems into Navision. Navision cash receipts are interfaced with the State's accounting system. DEQ implemented Navision in October 2004. Navision is managed by DEQ's OFM; however, the data is managed jointly by OFM and DEQ program divisions. As of June 2006, DEQ processed approximately $105 million in cash receipts and $53 million in invoices using Navision.

b. LABWORKS

LABWORKS is a laboratory information management system (LIMS) used to manage air, soil, water, oil, hazardous waste, sewage sludge, and brick and concrete samples for DEQ's environmental testing laboratories. The samples are managed in LABWORKS by DEQ's two environmental testing laboratories: the Drinking Water Laboratory and the Environmental Laboratory.

The Drinking Water Laboratory tests and analyzes the quality of drinking water, public swimming pool water, and public beach water and investigates the failures of sewage systems. The Drinking Water Laboratory serves DEQ, other State and federal agencies, and the general public. The Environmental Laboratory tests and analyzes organic and inorganic land, water, oil, and air samples for DEQ's environmental programs.

DEQ uses LABWORKS to log environmental and water samples, track sample results, validate samples, manage quality assurance, and report sample information. The Drinking Water Laboratory implemented LABWORKS in April 2005, and the Environmental Laboratory implemented LABWORKS in March 2003. LABWORKS tracks approximately 4.9 million test results on 99,000 samples each year.

c. Environmental Response Networked Information Exchange (ERNIE)

ERNIE is an information system used by DEQ's Remediation and Redevelopment Division to record, track, monitor, and report data related to incidents, facilities, and sites of environmental contamination in Michigan.

As of July 2006, the Division tracked 15,350 incidents; 9,626 facilities; and 8,252 sites in ERNIE. ERNIE was developed by a contractor in the 1990s. It is maintained by DIT.

Department of Information Technology (DIT)

DIT provides information support services to DEQ for Navision, LABWORKS, and ERNIE, including operating system configuration, application development and maintenance, database administration, program and data change controls, and backup and recovery controls.

Audit Objectives

Our performance audit* of Selected General and Application Controls, Department of Environmental Quality (DEQ) and Department of Information Technology (DIT), had the following objectives:

1. To assess the effectiveness* of DEQ and DIT's efforts in establishing appropriate security and access controls over data and data systems.

2. To assess the effectiveness of DEQ and DIT's efforts in establishing appropriate change management* controls over data and data systems.

3. To assess the effectiveness of DEQ and DIT's efforts in establishing appropriate backup and recovery controls over data and data systems.

4. To assess the effectiveness of DEQ and DIT's efforts to ensure the integrity* of data for Navision and LABWORKS.

Audit Scope

Our audit scope was to examine the information processing and other records of the Department of Environmental Quality's information systems. 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 procedures, performed from September 2005 through July 2006, included examination of records primarily for the period March 2003 through July 2006. We examined DEQ and DIT's efforts to establish appropriate security and access controls over data and data systems, change management controls, backup and recovery controls, and processing controls to ensure the integrity of Navision and LABWORKS.

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

To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We identified DEQ's data systems and assessed the risks* related to each system. We conducted a preliminary review of DEQ and DIT's information processing functions for administering access to data systems, maintaining security for production program and data files, and managing changes to production programs and data files. 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 general and application controls at DEQ. Specifically, we assessed:

   a. Security and Access Controls:

      (1) We examined and performed tests of management's access controls over Navision, LABWORKS, and the Environmental Response Networked Information Exchange (ERNIE).

      (2) We reviewed the security of network operating system configurations for Navision, LABWORKS, and ERNIE.

      (3) We evaluated the results of a vulnerability* scan of the network operating systems for Navision, LABWORKS, and ERNIE conducted with the assistance of DIT.

      (4) We reviewed network operating system administrative access for Navision, LABWORKS, and ERNIE.

   b. Change Management Controls:

      (1) We reviewed DIT policies and procedures for managing program and data changes.

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

(2) We reviewed and evaluated the effectiveness of DIT controls to ensure that approved changes are placed into production for Navision, LABWORKS, and ERNIE.

c. Backup and Recovery Controls:

(1) We interviewed DIT staff to obtain an understanding of backup and recovery controls over DEQ's information systems.

(2) We reviewed and evaluated server, database, and system backup and recovery procedures for Navision, LABWORKS, and ERNIE.

d. Integrity of Data in Navision and LABWORKS:

(1) We evaluated the effectiveness of controls over the integrity and completeness of data in Navision and LABWORKS and the associated risks.

(2) We obtained and reviewed customer, invoice, and deposit data within Navision for completeness and integrity. We obtained and reviewed sample data within LABWORKS for completeness and integrity.

(3) We assessed controls over the integrity and completeness of data transfers and batch processing within Navision.

3. Evaluation and Reporting Phase

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

We use a risk and opportunity based approach when selecting activities or programs to be audited. Accordingly, our audit efforts are focused on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. By design, our limited audit resources are used to identify where and how improvements can be made. Consequently, our performance audit reports are prepared on an exception basis.

Agency Responses

Our audit report contains 5 findings and 5 corresponding recommendations. DEQ's and DIT's preliminary responses indicate that they agree 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 agencies' written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require DEQ and DIT 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

SECURITY AND ACCESS

COMMENT

Background: Security controls include the implementation of policies, procedures, and guidelines to ensure the security of data. Access controls protect data from unauthorized modification, loss, or disclosure by restricting or detecting inappropriate access attempts. Effective controls include granting access to data and program files only to the extent necessary for individuals to perform their assigned duties.

Audit Objective: To assess the effectiveness of the Department of Environmental Quality (DEQ) and the Department of Information Technology's (DIT's) efforts in establishing appropriate security and access controls over data and data systems.

Conclusion: DEQ and DIT were not effective in their efforts to establish appropriate security and access controls over data and data systems. Our assessment disclosed one material condition*. DEQ, in conjunction with DIT, had not established and implemented an information systems security program and security and access controls over data and data systems (Finding 1). Our assessment also disclosed a reportable condition* related to server security (Finding 2).

FINDING

1. Security Program and Security and Access Controls

   DEQ, in conjunction with DIT, had not established and implemented an information systems security program and security and access controls over data and data systems. As a result, DEQ cannot ensure the security and integrity of its data.

   In Special Publication 800-53, the National Institute of Standards and Technology* (NIST) recommends that security controls should be employed as a part of a well-defined information systems security program. The security program is developed based on the results of comprehensive and periodic risk assessments* of data security needs. A comprehensive security program would also define and implement effective policies and procedures for granting access to data and data systems.

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

Our audit disclosed:

a. DEQ had not established a security officer position. A security officer would have the responsibility and authority to implement information security policies, standards, and operating procedures for safeguarding all data and data systems.

b. DEQ, in conjunction with DIT, did not restrict or establish compensating controls to detect system development staff access to production data. As a result, development staff could make unauthorized changes to data. We noted:

   (1) DEQ granted two DIT database administrators privileged access* to Navision.

   (2) DEQ granted a DIT developer privileged access to LABWORKS.

   (3) DEQ granted a DIT developer the responsibility for administering security and access to the Environmental Response Networked Information Exchange (ERNIE). In addition, DEQ granted one DIT database administrator privileged access to ERNIE.

   DEQ and DIT should restrict development staff from privileged access to production data because users with privileged access have the ability to bypass operating system and application security controls.

c. DEQ did not have policies and procedures to assign, restrict, and remove access to data. As a result, users were granted excessive access and could make unauthorized changes to Navision, LABWORKS, and ERNIE. We noted:

   (1) DEQ inappropriately assigned privileged access to six Navision users. In addition, DEQ assigned inappropriate access to five LABWORKS users, which allowed them to modify sample results.

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

(2) DEQ did not have a process to remove user access. We identified 7 users with Navision access and 28 users with ERNIE access who no longer required access to the systems.

Effective controls for assigning, restricting, and removing access would reduce the risk of unauthorized changes to data.

d. DEQ did not restrict privileged access to Navision and LABWORKS audit logs. In addition, DEQ did not monitor audit logs to detect unusual, high-risk, or inappropriate transactions. As a result, malicious or improper transactions could go undetected.

e. DEQ did not ensure that laboratory data changes could be made only through the LABWORKS application. Application security controls include logs that provide a record of data changes. As a result, privileged users had the ability to bypass application security controls and make changes to laboratory data.

f. DEQ and DIT did not encrypt password files in LABWORKS. As a result, privileged users had access to users' passwords.

RECOMMENDATION

We recommend that DEQ, in conjunction with DIT, establish and implement an information systems security program and security and access controls over data and data systems.

AGENCY PRELIMINARY RESPONSE

DEQ agrees and noted that the findings identify similar security weaknesses in several of DEQ's application systems. DEQ informed us that its security committee, established early in fiscal year 2005-06, recently issued a draft information security plan. The plan contains several recommended improvements for implementing an overall information security program, including establishment of a central security function/advisory team, establishment of new policies and procedures, and ongoing risk assessment practices. DEQ will implement plan recommendations in upcoming months and will determine appropriate resource alignments necessary to achieve outcomes identified in the plan.

DEQ informed us that, for ERNIE, it revoked user access for departed employees. DEQ also informed us that, for Navision, it implemented or plans to implement corrective actions including reaccrediting users, removing unnecessary user privileges, reassigning user security duties to a central security function for financial related systems within OFM, establishing user access forms, and refining the process of establishing and monitoring audit logs.

DEQ informed us that Laboratory management has restricted developer access to production data, completed reaccreditation of user privileges, and will annually reaccredit user privileges. DEQ also informed us that it received confirmation from the LABWORKS vendor that a future release of LABWORKS will encrypt passwords. In addition, Laboratory management will explore the benefit of additional corrective actions to restrict privileged user access to audit logs and to enhance monitoring activities. DEQ informed us that despite the conditions cited in the finding, Laboratory management believe that peer review activities are effective compensating controls to ensure data integrity.

FINDING

2. Server Security

DIT had not established effective security and access controls over the server operating systems*. As a result, DEQ's data was vulnerable to unauthorized modification, loss, or disclosure.

A well-secured server operating system helps provide a stable platform on which to run software. An operating system should be installed with a minimal service configuration to reduce the risk of network intrusion and the exploitation of well-known operating system vulnerabilities. In addition, the network administrator should routinely monitor log files for unauthorized access and other security related problems. We reviewed four servers that contain the Navision, LABWORKS, and ERNIE applications and databases. We noted:

a. DIT did not effectively manage privileged server user accounts. Privileged server user accounts allow a user full control of the network server operating

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

system. Therefore, administrative user accounts should be restricted and closely monitored. We noted:

(1) DIT did not remove eight privileged server user accounts for employees with changes in their job responsibilities.

(2) DIT did not remove two redundant privileged server user accounts.

(3) DIT did not ensure strong password controls for two privileged server user accounts.

b. DIT did not conduct periodic vulnerability scans to ensure the continued security of the server operating systems. We identified critical vulnerabilities in the operating system configuration of all four servers. Periodic vulnerability scans would help ensure that new threats* are identified and that critical security controls are in place.

c. DIT did not routinely monitor server operating system logs. As a result, the server operating systems are vulnerable to attacks that could compromise data, data systems, and the network.

RECOMMENDATION

We recommend DIT establish effective security and access controls over the server operating systems.

AGENCY PRELIMINARY RESPONSE

DEQ and DIT agree and DEQ will work with DIT to establish appropriate controls as part of implementing an information security plan. DIT informed us that it will continue to evaluate and implement reasonable cost-effective strategies that mitigate the level of risk to the server operating system. DIT informed us that it has started to strengthen controls by implementing security related modifications. Despite the noted risks, DIT informed us that it is not aware of any instances in which the confidentiality, integrity, or availability of DEQ information was compromised. DIT informed us that it will achieve full compliance by August 31, 2007.

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

CHANGE MANAGEMENT

COMMENT

Audit Objective: To assess the effectiveness of DEQ and DIT's efforts in establishing appropriate change management controls over data and data systems.

Conclusion: DEQ and DIT were not effective in their efforts to establish appropriate change management controls over data and data systems. Our assessment disclosed one material condition. DEQ and DIT had not established effective change management controls (Finding 3).

FINDING

3. Change Management Controls

DEQ and DIT had not established effective change management controls. As a result, DEQ and DIT cannot ensure that only authorized changes were made to data and data systems.

Effective change management controls should ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques to help ensure that all programs and program modifications are properly authorized, tested, and approved and that proper segregation of duties* exists.

Our review of change management controls disclosed:

a. DEQ and DIT did not test, approve, and document program changes. As a result, DIT cannot ensure that data systems work as intended and that only approved program changes were made.

b. DEQ and DIT did not ensure an appropriate segregation of duties for the change management process. As a result, unauthorized changes to data and data systems could go undetected. The DIT developer for ERNIE had full access to the production source code as well as the ability to move the source code into production. The Federal Information System Controls Audit Manual,

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

published by the U.S. Government Accountability Office, states that the ability to move changes into production should be the responsibility of a change control group independent of development staff.

c. DEQ and DIT did not maintain a log of all program changes. As a result, DIT cannot effectively monitor changes to DEQ's data systems. Program change logs provide an audit trail to ensure that program changes are authorized and approved by management.

RECOMMENDATION

We recommend DEQ and DIT establish effective change management controls.

AGENCY PRELIMINARY RESPONSE

DEQ and DIT agree and DEQ will work with DIT to establish appropriate controls as part of implementing an information security plan. DIT informed us that it has initiated a project to adapt its enterprise level change control process to the local change activities for its support areas. DIT also informed us that its support staff for DEQ is working with enterprise change managers to adapt and implement a Local Change Control Board with authority over DEQ information technology operations. DIT has informed us that it will achieve full compliance by September 30, 2007.

BACKUP AND RECOVERY

COMMENT

Audit Objective: To assess the effectiveness of DEQ and DIT's efforts in establishing appropriate backup and recovery controls over data and data systems.

Conclusion: DEQ and DIT were not effective in their efforts to establish appropriate backup and recovery controls over data and data systems. Our assessment disclosed a reportable condition related to backup and recovery controls (Finding 4).

FINDING

4. Backup and Recovery Controls

DEQ and DIT had not evaluated the criticality of DEQ's data and data systems to implement effective backup and recovery controls. As a result, DEQ and DIT cannot ensure the continuity of services and the recovery of critical data in the event of a disaster.

Our review of backup and recovery controls disclosed:

a. DEQ had not implemented a data classification process to identify critical data and data systems. As a result, DEQ cannot ensure that data is effectively protected and secured in the event of a business disruption. Control Objectives for Information and Related Technology* (COBIT) requires that data and data systems be protected and secured in a manner consistent with data classification categories. Data classification categories are defined by identifying the threats and vulnerabilities to business objectives in the event of a business disruption. DEQ has taken initial steps to quantify some threats to its systems in the biennial internal control evaluation process. However, to determine what data is critical in the event of a business disruption, DEQ should fully develop a data classification process.

b. DIT did not have a complete inventory of all the DEQ databases and data systems supported on its servers. DIT could not identify which databases and data systems were located on each server. Without identifying where databases and data systems are located, DIT cannot effectively manage and secure databases and data systems.

c. DEQ and DIT did not identify and prioritize critical data systems. As a result, DEQ cannot ensure that important services would not be disrupted in the event of a disaster. DEQ's Business Continuity Plan identifies the Drinking Water and Environmental Laboratories to be an agency critical function. However, DEQ has not identified any of its systems, including LABWORKS, to be supported by DIT without business interruption.

d. DIT did not test the backup files for DEQ databases and servers. As a result, DIT cannot ensure accurate, complete, and timely data restoration in the event

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

of a system failure or disaster. Backup and recovery procedures should include periodically testing the integrity of the backups.

RECOMMENDATION

We recommend that DEQ and DIT evaluate the criticality of DEQ's data and data systems to implement effective backup and recovery controls.

AGENCY PRELIMINARY RESPONSE

DEQ and DIT agree and informed us that they will work together to establish appropriate backup and recovery controls, including data classification, as part of implementing an information security plan. DIT informed us that it will work with DEQ to achieve full compliance by June 2007.

INTEGRITY OF DATA FOR NAVISION AND LABWORKS

COMMENT

Audit Objective: To assess the effectiveness of DEQ and DIT's efforts to ensure the integrity of data for Navision and LABWORKS.

Conclusion: DEQ and DIT were moderately effective in their efforts to ensure the integrity of data for Navision and LABWORKS. Our assessment disclosed a reportable condition related to data integrity (Finding 5).

FINDING

5. Data Integrity

DEQ did not fully ensure the integrity of data for Navision and LABWORKS.

Our review of Navision and LABWORKS disclosed:

a. DEQ did not ensure the accuracy and completeness of data in Navision.

Navision contains records of customers billed for permits, operating licenses, fees, registrations, civil fines, environmental cleanup settlements, training, water testing, and requests for information under the Freedom of Information

Act. We reviewed the Navision database for the period October 2004 through April 2006 and noted:

(1) DEQ did not fully ensure that the customer master file in Navision contained only one record per customer. We identified 2,474 duplicate customer records on Navision. Having more than one customer record could result in DEQ updating the inappropriate record. DEQ should develop controls to identify and prevent duplicate customer records.

(2) DEQ did not ensure that all customer records in Navision contained a payment term code. We noted 743 customer records with blank payment term codes. Establishing a payment term code for every customer record would help ensure accurate due dates and penalty amount calculations.

b. DEQ did not fully ensure the accuracy of environmental and water sample data within LABWORKS. Inaccurate data in LABWORKS could cause the reporting of incorrect sample test results.

DEQ samples and tests water from hazardous waste sites, rivers and lakes, and accidental spills of hazardous chemicals. The public relies on DEQ's Drinking Water and Environmental Laboratories to accurately test and report the presence of environmental contaminants. We reviewed the LABWORKS's water database for the period April 2005 through April 2006 and the LABWORKS's environmental database for the period March 2003 through April 2006 and noted:

(1) DEQ did not approve and monitor changes to formulas used to calculate sample test results. As a result, laboratory staff with access to the formulas could make unauthorized changes that could affect the accuracy of sample test results.

(2) DEQ did not ensure that LABWORKS edited data to detect sample date errors and did not qualify sample test results when required. Date errors inhibit DEQ's ability to test and report the sample test results. We identified 85 samples in which LABWORKS allowed laboratory staff to erroneously enter dates in an illogical sequence. In addition, we identified 49 samples in which DEQ did not test the sample by the required cut-off date for a reliable sample test result. DEQ did not send a disclosure

statement to the customer in these 49 instances. Laboratory practices require that DEQ send a disclosure statement to the customer qualifying the sample test result when a sample exceeds its cut-off time for a reliable test result.

(3) DEQ did not implement appropriate segregation of duties over the sample testing process. Also, DEQ did not have documented policies and procedures defining which phases of the sample validation process are incompatible. The validation process is a quality assurance function to confirm sample test results. We identified 37 samples for which one person acted as the analyst, analysis validator, and sample validator.

(4) DEQ did not fully ensure that accurate data fields existed in LABWORKS. Invalid data hinders DEQ's ability to use LABWORKS to manage and report LABWORKS information. We identified 16 environmental sites that had more than one location code. We also identified invalid data in 59 of 301 agency index codes and 67 of 218 agency program cost account codes. DEQ inputs codes into LABWORKS from documentation submitted by field staff without confirming the accuracy of the codes.

RECOMMENDATION

We recommend that DEQ fully ensure the integrity of data for Navision and LABWORKS.

AGENCY PRELIMINARY RESPONSE

DEQ agrees and informed us that, although some invalid data was identified during the audit, several of the data fields are used for informational purposes by DEQ program staff. DEQ informed us that, because of compensating controls, it believes that the impact to its processes is minor. However, the finding identified opportunities for improvement.

DEQ informed us that it has implemented or plans to implement corrective actions within the Navision and LABWORKS applications. For Navision, DEQ informed us that OFM developed an interface module to identify duplicate customer records prior to database updates. DEQ also informed us that OFM has communicated a new policy and provided user training requiring valid payment terms codes.

Further, OFM will consider requesting a change to the application so that the payment terms code is systematically required.

DEQ informed us that several of the invalid data conditions in LABWORKS involve very low error rates; however, Laboratory management is planning additional corrective actions. DEQ informed us that Laboratory management redesigned Laboratory practices to ensure segregation of duties and enhanced its peer review process to monitor data integrity. Laboratory management will explore alternative approaches to monitoring critical data changed external to LABWORKS. In addition, DEQ informed us that Laboratory management has implemented monitoring reports to identify inconsistent/invalid data for use in correcting data before a sample process is closed.

GLOSSARY

change management	A control system that ensures that programs, systems, and infrastructure modifications are authorized, tested, documented, and monitored.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines developed by the Information Systems Audit and Control Foundation (ISACF) as a generally applicable and accepted standard for good practices for controls over information technology.
DEQ	Department of Environmental Quality.
DIT	Department of Information Technology.
effectiveness	Program success in achieving mission and goals.
ERNIE	Environmental Response Networked Information Exchange.
integrity	The accuracy, completeness, and timeliness of data in an information system.
LIMS	laboratory information management system.
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.
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 systems.

OFM	Office of Financial Management.
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 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, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
risk	The probability that a particular security threat will exploit a system vulnerability.
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.
segregation of duties	Separation of the management or execution of certain duties or areas of responsibility in order to prevent and reduce opportunities for unauthorized modification or misuse of data or service.
server operating system	The software that manages the application and data files that are shared over a network.

threat	An activity, intentional or unintentional, with the potential for causing harm to an information system or activity.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL