MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF THE

ENTERPRISE DATA WAREHOUSE

DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

August 2014

Doug A. Ringler, C.P.A., C.I.A.
AUDITOR GENERAL

071-0520-14

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

Enterprise Data Warehouse

Department of Technology, Management, and Budget

Report Number:
071-0520-14

Released:
August 2014

The Enterprise Data Warehouse (EDW) is a centralized repository of historical data that is used to support State agencies' decision-making and business processes. The Department of Technology, Management, and Budget (DTMB), in conjunction with State agencies, extracts data from source systems, transforms it into the proper format, and loads it into the EDW. State agencies use analytical tools to query data stored on the EDW to generate State and federal reports, project State revenues, perform trend analyses, and detect fraud.

Audit Objective	Audit Conclusion
Objective 1: To assess the effectiveness of the State's efforts to ensure the reliability of data in the EDW.	Not effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB, in conjunction with State agencies, had not fully established effective interface controls over the EDW (Finding 1).	X		Agree
DTMB, in conjunction with State agencies, had not established an effective governance structure over the EDW (Finding 2).		X	Agree

Audit Objective	Audit Conclusion
Objective 2: To assess the effectiveness of the State's efforts to implement user access controls over the EDW.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
State agencies, in conjunction with DTMB, had not fully established and implemented effective user access controls over the EDW (Finding 3).		X	Agree
DTMB, in conjunction with State agencies, had not fully established and implemented effective access controls over temporary privileged accounts (Finding 4).		X	Agree

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

Doug A. Ringler, C.P.A., C.I.A.
Auditor General

Laura J. Hirst, C.P.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

DOUG A. RINGLER, C.P.A., C.I.A.
AUDITOR GENERAL

August 19, 2014

Mr. David B. Behen
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Mr. Behen:

This is our report on the performance audit of the Enterprise Data Warehouse, Department of Technology, Management, and Budget.

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

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agency's response at the end of our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

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

Sincerely,

Doug Ringler

Doug Ringler, C.P.A., C.I.A.
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

ENTERPRISE DATA WAREHOUSE
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

Description

The Enterprise Data Warehouse (EDW) is a centralized repository of historical data that is used to support State agencies' decision-making and business processes (see illustrations on pages 7 and 8). Three executive branch departments (the Department of Community Health [DCH], Department of Human Services [DHS], and Department of Treasury [Treasury]) and the State Court Administrative Office (SCAO), within the judicial branch, actively load data directly into the EDW production environment. The process for transmitting data to the EDW includes extracting the data from source systems, transforming the data into the proper format, and then loading the data into the EDW.

At the time of our review, there were over 2,600 active EDW users, made up of State employees, local government employees, and third parties. The EDW consisted of over 9,600 production tables containing over 121.5 billion rows of data. Much of the data stored on the EDW is sensitive or confidential. For example, the EDW contains client and payment data for certain large public assistance programs such as Medicaid, State and federal tax return data, vital records data, Michigan court and offender data, and child support enforcement data. State agencies use analytical tools to query data stored on the EDW to generate State and federal reports, project State revenues, perform trend analyses, and detect fraud.

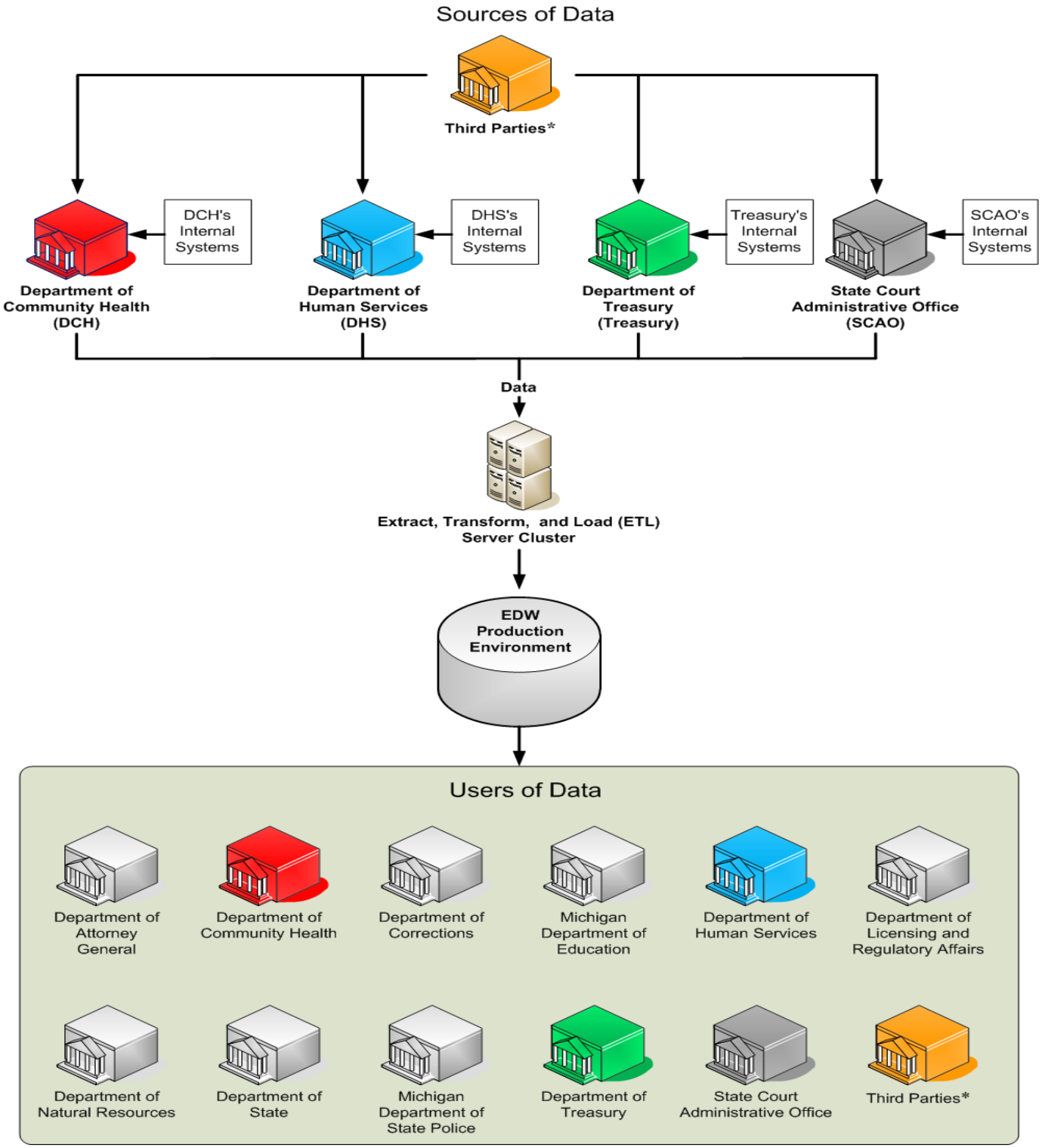
Data Center Operations, within the Department of Technology, Management, and Budget (DTMB), is responsible for the configuration, support, and maintenance of the EDW operating system* and database management system*. DTMB Customer Services and third party vendors manage the design and development of the EDW environment for the executive branch agencies (i.e., DCH, DHS, and Treasury). In addition, Customer Services and third party vendors load executive branch agency data into the EDW. EDW database* design and development for the judicial branch (i.e., the SCAO) are performed by a third party vendor. The third party vendor is also responsible for loading judicial data into the EDW.

In fiscal year 2012-13, DTMB billed the four State agencies $8.1 million for costs related to EDW usage and data storage.

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

Illustration 1

Enterprise Data Warehouse (EDW)
Sources and Users of Data

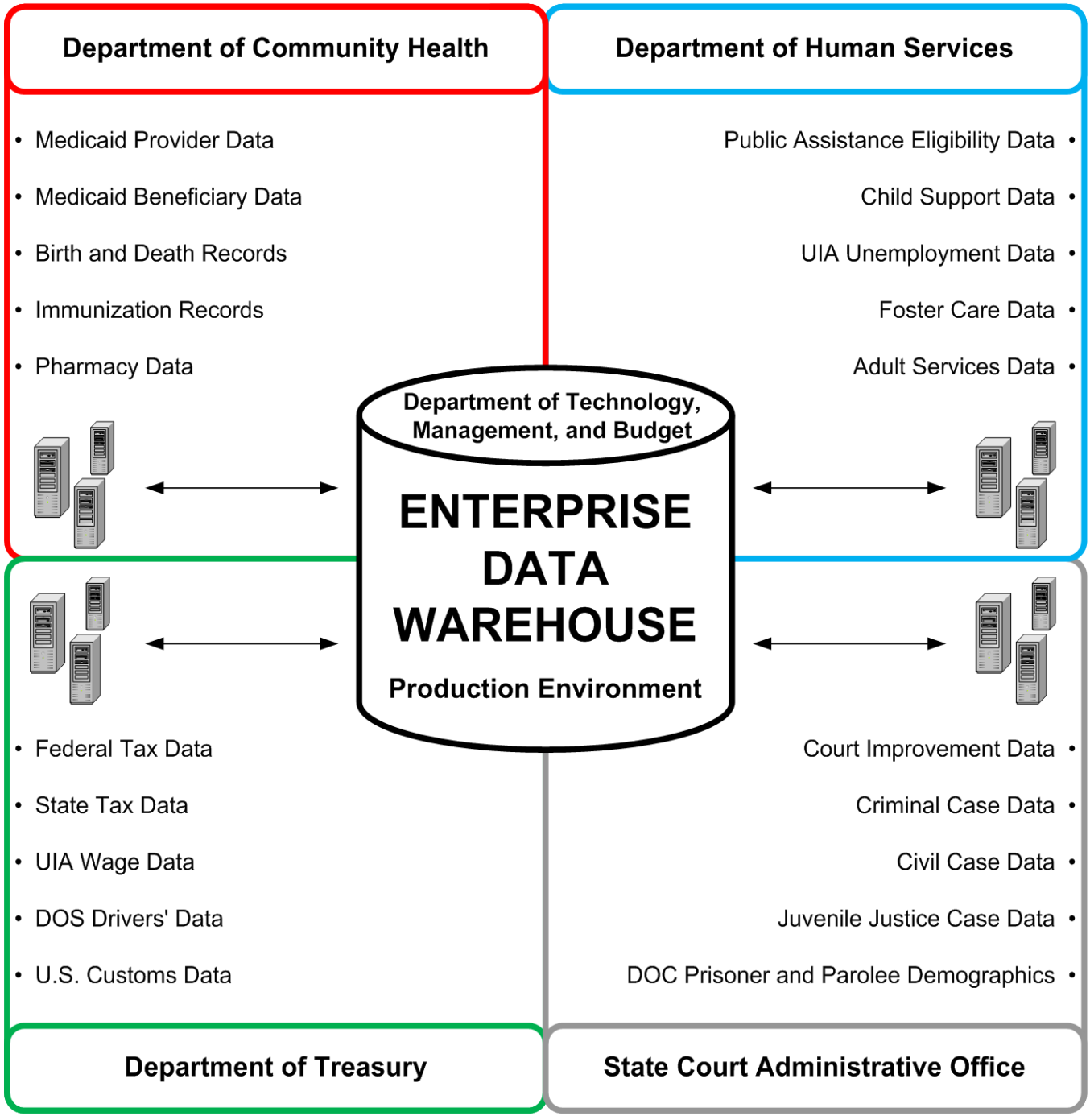


*Third Parties could include State departments, federal agencies, local agencies, and private organizations.

Source: Prepared by the Office of the Auditor General from information and documentation provided by the Department of Technology, Management, and Budget.

Illustration 2

Enterprise Data Warehouse (EDW)
Examples of Data Stored on the EDW



Source: Prepared by the Office of the Auditor General from information and documentation provided by the Department of Technology, Management, and Budget.

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of the Enterprise Data Warehouse (EDW), Department of Technology, Management, and Budget (DTMB), had the following objectives:

1. To assess the effectiveness* of the State's efforts to ensure the reliability* of data in the EDW.

2. To assess the effectiveness of the State's efforts to implement user access controls* over the EDW.

Audit Scope

Our audit scope was to examine the State's efforts to ensure the reliability of data and implement user access controls over the Enterprise Data Warehouse. We did not conduct tests of the accuracy of data within the Enterprise Data Warehouse; therefore, we make no conclusions regarding the accuracy of the data. However, our audit disclosed a material condition* related to interface 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, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered the period October 1, 2012 through June 30, 2014.

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* (FISCAM), the National Institute of Standards and Technology* (NIST), DTMB policies and procedures, and other information security* and industry best practices.

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

We conducted a preliminary survey of controls over the EDW production environment, including interface controls, access controls, and governance structure, specific to the four agencies that load data into the EDW. We interviewed DTMB, the four State agencies that load data into the EDW, and third party vendors to obtain an understanding of the type of data being loaded into the EDW, the importance of the data, and the management and control structure specific to the four EDW environments. We used the results of our preliminary survey to determine the extent of our detailed analysis and testing.

To accomplish our first audit objective, we:

- Identified the interface processes that load critical data into the EDW and the table views of critical data stored on the EDW.

- Reviewed the governance structure over the EDW.

- Judgmentally selected 100 critical interfaces and tested selected controls, such as interface strategy and design, reconciliation controls, and error handling procedures.

- Judgmentally selected and tested 107 table views to ensure that the information being displayed by the views came from the EDW production environment and that user acceptance testing was performed.

- Reviewed and assessed DTMB's standards and guidance for data sharing.

- Reviewed partnership agreements between DTMB and the State agencies.

- Judgmentally selected and reviewed 8 data sharing agreements to determine if the agreements contained industry recommended provisions, such as security requirements over transferred data; method of data transfer; error notification requirements; and responsibilities for the completeness, accuracy, and timeliness of shared data.

To accomplish our second audit objective, we:

- Interviewed DTMB and State agency staff to gain an understanding of the process for granting and monitoring user and temporary privileged account* access to the EDW.

- Judgmentally selected 117 users and reviewed the appropriateness of their access to EDW data.

- Reviewed and assessed the periodic recertification of user access rights performed by the State agencies.

- Randomly selected and tested 65 temporary privileged accounts to ensure that activity logs were maintained and monitored and that the use of the accounts was approved for a valid business purpose.

We judgmentally selected the interfaces and table views for testing based on their criticality to agency operations.

We based our conclusions on our audit efforts as described in the preceding paragraphs and the resulting material condition and reportable conditions* noted in the comments, findings, recommendations, and agency preliminary responses section. In our professional judgment, the material condition is more severe than a reportable condition and could impair management's ability to operate effectively or could adversely affect the judgment of an interested person concerning the effectiveness of the EDW. The reportable conditions are less severe than a material condition but represent deficiencies in internal control.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve the operations of State government. Consequently, we prepare our performance audit reports on an exception basis.

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

Agency Responses

Our audit report contains 4 findings and 4 corresponding recommendations. DTMB and other State agencies' preliminary response indicates that they agree with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion at the end of 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 DTMB to develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF EFFORTS TO ENSURE RELIABILITY OF DATA IN THE EDW

COMMENT

Audit Objective: To assess the effectiveness of the State's efforts to ensure the reliability of data in the Enterprise Data Warehouse (EDW).

Audit Conclusion: We concluded that the State's efforts to ensure the reliability of data in the EDW were not effective.

Factors leading to this conclusion included the:

- Critical nature of the interfaces tested and the impact of exceptions noted on the accuracy and reliability of the data stored in the EDW.

- Number of entities using and relying on EDW data for decision-making and for State and federal reporting.

- Material condition and reportable condition related to interface controls over the EDW and the governance structure over the EDW, respectively.

FINDING

1. Interface Controls

   The Department of Technology, Management, and Budget (DTMB), in conjunction with State agencies, had not fully established effective interface controls over the EDW. As a result, interfaces may not be designed to ensure that data is transferred completely, accurately, and timely from the source systems to the EDW.

   According to the U.S. Government Accountability Office's (GAO's) Federal Information System Controls Audit Manual (FISCAM), controls surrounding interface processing should reasonably ensure that data is transferred from the source system to the target system completely, accurately, and timely.

We reviewed interface controls for 100 judgmentally selected interfaces. Our review disclosed:

a. DTMB, in conjunction with State agencies, did not always implement an effective interface strategy or interface design for each EDW interface.

According to FISCAM, an interface strategy should be developed to keep data synchronized between a source system and a target system. The interface strategy should include the following elements: an explanation of each interface, the interface method chosen, the data fields being interfaced, the controls to reasonably ensure that the data is interfaced completely and accurately, timing requirements, assignment of responsibilities, ongoing system balancing requirements, and security requirements. Interface design documentation, such as data mapping tables that describe how data is transformed between a data source and destination, validations and edits, roles and responsibilities for the interface process, and error correction and communication methods, should also be developed for each interface.

We noted that DTMB and the State agencies had no documentation of their interface strategy or interface design for 36 of the 100 interfaces and had incomplete documentation for 50 of the 100 interfaces. The following table summarizes the results of our review by agency:

State Agency EDW Environment	Number of Interfaces		
	Reviewed	With No Strategy or Design Documentation	With Incomplete Strategy or Design Documentation
Department of Community Health (DCH)	25	0	25
Department of Human Services (DHS)	25	25	0
State Court Administrative Office (SCAO)	25	0	25
Department of Treasury (Treasury)	25	11	0
Total	100	36	50

b. DTMB, in conjunction with State agencies, did not implement effective interface reconciliation controls for 64 of the 100 interfaces tested.

According to FISCAM, interface reconciliation controls between a source system and a target system, such as the use of control totals, record counts, hash totals, or batch run totals, would help ensure the complete and accurate transfer of data. For the 64 interfaces without effective reconciliation controls, we noted instances in which interface activity was not logged, instances in which interface audit logs did not capture sufficient control totals, and instances in which interface control totals were sufficiently captured but no reconciliation control had been implemented to ensure that data transferred completely and accurately from the source system to the EDW. The following table summarizes interface reconciliation controls by agency:

State Agency EDW Environment	Number of Interfaces Reviewed	Number of Interfaces Without Effective Reconciliation Controls
DCH	25	5
DHS	25	22
SCAO	25	25
Treasury	25	12
Total	100	64

Interface controls were not fully established over the EDW because DTMB had not established effective policies and procedures to manage interfaces, such as guidance for interface strategy and design documentation, interface reconciliation controls, and audit logs.

RECOMMENDATION

We recommend that DTMB, in conjunction with State agencies, fully establish effective interface controls over the EDW.

AGENCY PRELIMINARY RESPONSE

DTMB, in conjunction with State agencies, agrees with the recommendation.

DTMB informed us that it will update its Enterprise Data Warehouse Guidelines for Best Practices to include new recommendations for interface controls. The document's Extract, Transform, and Load (ETL) Best Practices section will include strategy, design, and reconciliation controls that are in accordance with FISCAM.

DTMB also informed us that it will partner with DHS to create an interface strategy and design for each DHS EDW interface and that all new tables will have documentation for interface and design. In addition, the departments will ensure that effective controls are in place between the source and target systems, such as control totals, record counts, hash totals, and batch run totals. DTMB will also partner with DCH and the DCH data warehouse vendor to update interface documentation where gaps exist.

In addition, DTMB informed us that, prior to the start of the audit, Treasury had identified interface controls as an area for improvement and had begun working with DTMB to ensure that control reports are available and legacy (mainframe) data is transferred completely, accurately, and timely to the data warehouse. Treasury and DTMB are already working on a reconciliation process that will be applied across all interfaces moving data to Treasury's EDW environment.

FINDING

2. Governance Structure

DTMB, in conjunction with State agencies, had not established an effective governance structure over the EDW. As a result, DTMB, in conjunction with State agencies, could not ensure that the EDW environment is appropriately managed and secured. Findings 1, 3, and 4 resulted from a lack of fully established policies and procedures that should be established within a governance structure.

DTMB, as the EDW service provider and data custodian, is responsible for the establishment of an EDW governance structure. An information security governance structure should be established through policy development and is necessary for identifying the roles and responsibilities related to the management and oversight of the EDW.

Our review of the EDW governance structure disclosed:

a. DTMB, in conjunction with State agencies, did not define within the partnership agreements the roles and responsibilities of those charged with governance over the EDW. As a result, roles and responsibilities were not clearly communicated, which could lead to misunderstandings between DTMB and the State agencies regarding the delineation of duties and business owners' expectations.

   According to National Institute of Standards and Technology (NIST) Special Publication 800-35, partnership agreements should specify the services being provided and make all parties aware of their roles, responsibilities, and performance expectations for information technology* services that are provided.

   We reviewed the partnership agreements between DTMB and the State agencies utilizing the EDW production environment. We noted that clearly defined roles and responsibilities for the management of the EDW were not included within all three partnership agreements reviewed (DCH, DHS, and Treasury). We also noted that DTMB and the SCAO had not established a partnership agreement.

b. DTMB had not established clear guidance on the necessary provisions to be included in data sharing agreements. Clear guidance would help prevent shared data from being misused and help mitigate miscommunication of roles and responsibilities between data providers and recipients.

   Executive Directive No. 2013-1 states that all State departments and agencies must work in partnership with DTMB to establish the procedures and protocols for cross-departmental and jurisdictional data sharing and processing. According to NIST Special Publication 800-47, an agreement should be established between respective parties when sharing data and information resources.

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

We judgmentally selected eight data sharing agreements to review. We determined that the data sharing agreements did not include necessary information for securing shared data as well as defining the roles and responsibilities of all parties. For instance, the data sharing agreements did not consistently include provisions such as cost considerations, how long data can be retained after termination of the agreement, authority to conduct audits, restrictions on the disclosure of information, security requirements over transferred data, method of data transfer, notification requirements if the data transfer method changes or an error in shared data is identified, and responsibilities for the completeness, accuracy, and timeliness of shared data.

In our November 2005 performance audit of the State's Teradata data warehouse, we reported that DTMB had not established standards for data sharing agreements. DTMB indicated that standards for data sharing agreements were an integral part of its overall data warehouse strategy. DTMB also indicated that it would develop data sharing standards as part of its data warehouse strategy, which it expected to implement in fiscal year 2006-07. However, DTMB had not developed and implemented data sharing standards.

DTMB informed us that the cause of the issues was a lack of direction for the authority over governance until the Governor, in November 2013, issued Executive Directive No. 2013-1.

RECOMMENDATION

We recommend that DTMB, in conjunction with State agencies, establish an effective governance structure over the EDW.

AGENCY PRELIMINARY RESPONSE

DTMB, in conjunction with State agencies, agrees with the recommendation.

DTMB informed us that it established an Enterprise Information Management (EIM) Steering Committee in response to Executive Directive No. 2013-1, which is composed of eight departments that are currently engaged in numerous aspects of data sharing. The EIM Steering Committee is in the process of founding the EIM program, including a legal framework, roles and responsibilities, organizational

processes, data governance framework, and a data sharing template. The EIM program will be presented to the Michigan Information Management Governing Board, composed of directors or chief deputy directors of all State departments, for its review and approval. DTMB, in coordination with EIM, will develop a data sharing agreement template for use among State agencies. In addition, DTMB will work to establish procedures and protocols for cross departmental and jurisdictional data sharing.

Also, DTMB informed us that, prior to the start of the audit, Treasury established a governance structure, which is defined in the Treasury Data Governance Program Charter, identifying and defining the roles of the executive sponsors, Data Governance Steering Committee, Projects and Process Sub-Committee, and Data Governance User Group. Going forward, Treasury will add Appendix K for the Treasury EDW environment to its partnership agreement with DTMB to address the roles and responsibilities between an agency and DTMB, problem management and escalation, as well as baseline service level targets.

EFFECTIVENESS OF EFFORTS TO IMPLEMENT USER ACCESS CONTROLS OVER THE EDW

COMMENT

Audit Objective: To assess the effectiveness of the State's efforts to implement user access controls over the EDW.

Audit Conclusion: We concluded that the State's efforts to implement user access controls over the EDW were moderately effective.

Factors leading to this conclusion included the:

- Sensitivity and confidentiality* of data stored on the EDW.
- Historical nature of the data.

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

- Extent of access privileges granted to users.

- Reportable conditions related to user access controls and temporary privileged account access controls.

FINDING

3. User Access Controls

State agencies, in conjunction with DTMB, had not fully established and implemented effective user access controls over the EDW. Fully established and implemented user access controls would help prevent or detect inappropriate access to and modification of EDW data.

DTMB Administrative Guide policy 1335 requires the establishment of a process for controlling and documenting the allocation of user access rights based upon the principle of least privilege*. In addition, policies should be established to allow access to be managed, controlled, and periodically reviewed to ensure that user access is based on current job responsibilities.

Our review of selected access controls disclosed:

a. State agencies, in conjunction with DTMB, had not fully established and implemented effective user access controls for granting user access rights. Implementing effective access controls would help prevent unauthorized access and granting of privileges beyond what is necessary for a user's job responsibilities.

We reviewed access request forms for 117 judgmentally selected users who had access to the EDW production data. We noted:

(1) State agencies had not designed effective access request forms. We noted that, in the DHS and Treasury EDW environments, access request forms were not designed to include a user's access rights. As a result, these State agencies were unable to effectively ensure that access rights granted to users were approved and appropriate for their job responsibilities.

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

(2) State agencies, in conjunction with DTMB, did not restrict user access rights based upon the principle of least privilege. We noted that, in DHS and Treasury EDW environments, 16 users were granted high-risk user access rights. As a result, these State agencies could not ensure that users were not inappropriately modifying production data.

These high-risk user access rights allow these 16 users to modify (insert, update, or delete) production data within their environment. The EDW contains production data from various source systems. Modification of the EDW production data should be controlled and monitored using the temporary privileged account process. The following table summarizes the high-risk users by agency:

State Agency EDW Environment	Number of Users With High-Risk Access Rights
DCH	0
DHS	14
SCAO	0
Treasury	2
Total	16

(3) State agencies, in conjunction with DTMB, did not always document their approval of access granted to users. Of 117 users reviewed, 10 users did not have an access request form and 51 users had access to data that was not approved on their access request form. Documenting the authorization of user access helps to ensure that only appropriate

individuals have access to EDW and that their level of access is appropriate. The following table summarizes these users by agency:

State Agency EDW Environment	Number of Users		
	Reviewed	Without Access Request Forms	With Unapproved Access to Data
DCH	25	5	2
DHS	25	5	16
SCAO	25	0	0
Treasury	42	0	33
Total	117	10	51

(4) DTMB did not ensure that the PUBLIC account was restricted from having unnecessary access rights to system tables containing metadata* and user data as noted in part b.(2) of this finding. The PUBLIC account is a high-risk account because any rights that are granted to the PUBLIC account are automatically inherited by all users. As a result, all users in the EDW environment inherited unnecessary access rights that increased the vulnerability* of system security in the EDW.

b. State agencies, in conjunction with DTMB, had not fully established and implemented controls for periodically reviewing EDW user access rights. Without a periodic review of user access rights, State agencies cannot ensure that users' levels of access remain appropriate for their job responsibilities. Our review of user access rights disclosed:

(1) DCH, DHS, and the SCAO did not perform a periodic review of user access rights granted to individuals with access to their EDW data.

(2) DTMB did not perform a periodic review of the access rights granted to the PUBLIC account. After we brought this matter to management's attention, DTMB reviewed the access rights granted to the PUBLIC account and identified 186 access rights that users did not need to perform their job responsibilities.

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

User access controls were not fully established and implemented because State agencies had not designed effective policies and procedures governing the granting and periodic review of user access rights.

RECOMMENDATION

We recommend that State agencies, in conjunction with DTMB, fully establish and implement effective user access controls over the EDW.

AGENCY PRELIMINARY RESPONSE

State agencies, in conjunction with DTMB, agree with the recommendation and will work together to improve user access controls over the EDW.

DTMB informed us that the departments have already restricted or revoked the user access rights for those users identified in the audit report who did not require the access rights to complete their job responsibilities. The departments are working to revise access request forms, ensure that appropriate access rights are granted and periodically reviewed, and ensure that approvals are captured and documented. DTMB's Enterprise Data Warehouse Guidelines for Best Practices will provide agencies with guidelines to perform periodic reviews to verify that appropriate privileges are granted to authorized users. In addition, DTMB will analyze the access rights associated with the PUBLIC account and will restrict the rights to ensure that they comply with the principle of least privilege. All access rights associated with the PUBLIC account will be reviewed periodically.

DCH also informed us that it performs periodic reviews of user access controls, including a full review which was conducted in 2012. However, DCH acknowledged that its policy does not stipulate the frequency of the periodic reviews. DCH will modify its policy to incorporate periodic reviews of EDW access rights. Also, DCH's Database Security Application functionality is being enhanced to include automatically initiated renewal requests for users on an annual basis.

FINDING

4. Temporary Privileged Account Access Controls

DTMB, in conjunction with State agencies, had not fully established and implemented effective access controls over temporary privileged accounts.

Without effective controls, DTMB and State agencies cannot ensure that temporary privileged accounts are not used to inappropriately access or modify EDW data that is used for State and federal reporting, State revenue forecasting, client eligibility determinations, and many other critical functions.

DTMB Technical Standard 1335.00.03 requires that processes be established for managing and monitoring accounts.

Temporary privileged accounts provide system developers and database administrators* with high-risk access rights that allow them to change data, the database structure, or the database configuration. We randomly selected 65 of 614 temporary privileged accounts. Our review of selected access controls over the temporary privileged accounts disclosed:

a. DTMB, in conjunction with State agencies, did not authorize 60 of the 65 temporary privileged accounts. Without proper authorization, DTMB and State agencies cannot ensure that temporary privileged accounts are granted to appropriate users for valid business purposes. The following table summarizes the results of our review of temporary privileged accounts by agency:

State Agency EDW Environment	Temporary Privileged Accounts	
	Reviewed	Not Approved
DCH	25	25
DHS	25	25
SCAO	10	10
Treasury	5	0
Total	65	60

b. DTMB, in conjunction with State agencies, did not monitor the use of temporary privileged accounts. Our review disclosed that temporary privileged account activity was not monitored in any of the four EDW environments reviewed. Without monitoring, DTMB and State agencies could not ensure that the use of these accounts was appropriate and that no unauthorized changes were made to EDW data, the database structure, or the database configuration.

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

Access controls over temporary privileged accounts were not fully established and implemented because DTMB, in conjunction with the State agencies, had not designed effective policies and procedures to authorize and monitor temporary privileged accounts.

RECOMMENDATION

We recommend that DTMB, in conjunction with State agencies, fully establish and implement effective access controls over temporary privileged accounts.

AGENCY PRELIMINARY RESPONSE

DTMB, in conjunction with State agencies, agrees with the recommendation.

DTMB informed us that it will establish an automated centralized process to facilitate the authorization and review of temporary privileged accounts. DTMB will work with State agencies to develop a process and mechanism for properly authorizing privileged account access for State employees and third party contractors and vendors. In addition, DTMB's Enterprise Data Warehouse Guidelines for Best Practices will provide State agencies with guidelines for reviewing and monitoring temporary privileged accounts. Lastly, Treasury is in the process of implementing procedures for the approval and monitoring of temporary privileged accounts.

GLOSSARY

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
confidentiality	Protection of data from unauthorized disclosure.
database	A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection information that serves the purposes qualifies as a database, even if the information is not stored on a computer.
database administrator	The person 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.
DCH	Department of Community Health.
DHS	Department of Human Services.
DOC	Department of Corrections.
DOS	Department of State.

DTMB	Department of Technology, Management, and Budget.
EDW	Enterprise Data Warehouse.
effectiveness	Success in achieving mission and goals.
EIM	Enterprise Information Management.
Federal Information System Controls Audit Manual (FISCAM)	A methodology published by the U.S. Government Accountability Office (GAO) for performing information system control audits of federal and other governmental entities in accordance with *Government Auditing Standards*.
information technology	Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources.
interface controls	Controls that ensure the accurate, complete, and timely processing of data exchanged between information systems.
material condition	A matter that, in the auditor's judgment, is more severe than a reportable condition and 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.
metadata	Information about data within the data warehouse. This includes descriptions of the sources for the data; the description of each field; the procedures required to move the data from operational systems to the warehouse; and other operational information, such as the history of the migrated data, what organizational unit is responsible for a given field,

	what happens to the data during migration, what data has been purged, what data is due to be purged, and who is using the data and how they are using it.
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.
operating system	The essential program in a computer that manages all the other programs and maintains disk files, runs applications, and handles devices such as the mouse and printer.
performance audit	An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.
principle of least privilege	The practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.
privileged account	An account that has access to all commands and files on an operating system or database management system.
reliability	The accuracy and completeness of computer-processed data.

reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and 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 audit objectives; 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.
SCAO	State Court Administrative Office.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
Treasury	Department of Treasury.
UIA	Unemployment Insurance Agency.
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


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL