Office of the Auditor General
Performance Audit Report

Records Management

Records Management Services
Department of Technology, Management, and Budget

November 2016

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

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

Performance Audit

Records Management

Records Management Services (RMS) Department of Technology, Management, and Budget

Report Number:
071-0835-16

Released:
November 2016

RMS provides assistance to State and government agencies with managing records. Services include evaluating records management options, providing training to State agencies, developing retention and disposal schedules, operating the State Records Center, and administering the State of Michigan's master contracts for microfilming and digital imaging services.

Audit Objective			Conclusion
Objective #1: To assess the effectiveness of RMS's security and access controls over document management systems.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
RMS did not fully establish and implement security and access controls over its primary information technology systems to ensure the authorization and authentication of users and the protection of data. RMS did not disable user accounts for departed or transferred users and did not require complex passwords (Finding #1).		X	Agrees

Audit Objective			Conclusion
Objective #2: To assess the effectiveness of RMS's efforts to safeguard confidential information.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
RMS needs to improve its safeguards for confidential information to minimize the likelihood that confidential data could be accessed by unauthorized personnel. RMS stores all records in a similar manner, regardless of confidentiality or sensitivity, with many individuals having access to stored records without a business need for such access (Finding #2).		X	Agrees

Audit Objective	Conclusion
Objective #3: To assess RMS compliance with retention and disposal schedules.	Complied, with exceptions

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
RMS did not ensure the entry of necessary information into Versatile to calculate destruction dates, resulting in State records that may be retained beyond their approved destruction time period. We identified 23,728 boxes of records that may never be subject to destruction (Finding #3).		X	Agrees
RMS did not ensure that State agencies incorporated records created electronically, including the underlying data that supports electronic records, into retention and disposal schedules. Electronic records should be subject to the same review and approval processes as physical records (Finding #4).		X	Agrees

Audit Objective	Conclusion
Objective #4: To assess the effectiveness of RMS's monitoring of records management contracts.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
RMS did not always monitor its records management contracts to help ensure vendor compliance regarding damaged, lost, or improperly imaged records. Two contracts accounted for $7.7 million in expenditures during our audit period (Finding #5).		X	Agrees

November 10, 2016

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:

I am pleased to provide this performance audit report on Records Management, Records Management Services, Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agency provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and submit it within 60 days of the date above 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
Auditor General

TABLE OF CONTENTS

RECORDS MANAGEMENT

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

SECURITY AND ACCESS CONTROLS

BACKGROUND	Security and access controls limit or detect inappropriate access, which is important to ensure the availability, confidentiality, and integrity of records*.
	Versatile* is the records management software system used by Records Management Services (RMS) to manage record boxes stored at the State Records Center*. State agencies use Versatile to record the submission and retrieval of boxes and files. The Image Repository for Michigan Agencies* (IRMA) is a digital image storage and retrieval service offered to State agencies. Records Manager* is a document management solution that State agencies use to centrally manage electronic records, regardless of format.
	Department of Technology, Management, and Budget (DTMB) policies establish Statewide information technology policies, standards, and procedures.
AUDIT OBJECTIVE	To assess the effectiveness* of RMS's security and access controls over document management systems.
CONCLUSION	Moderately effective.
FACTORS IMPACTING CONCLUSION	• IRMA and Records Manager require complex passwords and periodic password expirations.
	• RMS coordinates semiannual Records Manager audits to ensure appropriate user access.
	• Reportable condition* related to improving system security and access controls (Finding #1).

See glossary at end of report for definition.

FINDING #1

Improvements needed to system security and access controls.

RMS did not fully establish and implement security and access controls over the Versatile and IRMA systems to ensure the authorization and authentication of users and the protection of data.

Our review of the three document management systems (Versatile, IRMA, and Records Manager) disclosed that RMS did not:

- Disable user accounts that no longer required access to Versatile or IRMA:

    o Of the 1,484 Versatile users, 249 (17%) last logged in before fiscal year 2014. An additional 171 (12%) users had never logged in since access was granted.

    o Our review of 60 randomly selected Versatile users identified 8 (13%) users who still had access even though they were no longer employed by the State, had transferred to another State department, or had changed job duties.

    o We randomly selected 60 of the 1,194 IRMA users and identified 3 (5%) users who still had access even though they either were no longer employed by the State or had transferred to another State department.

    DTMB Technical Standard 1335.00.03 requires RMS to review accounts every 120 days and deactivate accounts of terminated or transferred users. RMS sends agency records management officers the current user access lists semiannually to determine their continued accuracy. However, RMS did not review the accounts nor did it require a response back from the agencies to ensure the completion of the reviews.

- Utilize complex passwords and periodic password expirations in Versatile. RMS was not aware that Versatile could accept complex passwords.

    DTMB Technical Standard 1335.00.03 requires a system to enforce minimum password complexities of containing at least eight characters with three different categories of characters. The Standard also requires a maximum lifetime of 90 days for a password.

RECOMMENDATION

We recommend that RMS fully establish and implement security and access controls to properly protect the Versatile and IRMA systems and data.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees and will comply with the recommendation. RMS is working with agency records management officers to improve security and access controls and has already increased the frequency of the review of user accounts. To improve the Versatile system's security and access controls, RMS will notify users, when new accounts are created and/or passwords are reset, that the password must comply with State standards. While neither the current version nor the next version of Versatile has the capability to systematically require complex passwords, we will encourage staff to utilize complex passwords to the extent they are available in Versatile. DTMB will decommission the IRMA system by December 2016. All IRMA data and documents will be migrated to other systems, such as Records Manager and the State's Enterprise FileNet solution.

SAFEGUARDING OF CONFIDENTIAL INFORMATION

BACKGROUND

RMS provides the Department of Treasury (Treasury) with storage for active files through a service level agreement (SLA). The SLA requires RMS employees handling potentially confidential data to complete confidentiality training and an agreement annually. Completing the training and agreement ensures that employees are aware of and will abide by the rules and regulations related to Treasury's confidential data.

AUDIT OBJECTIVE

To assess the effectiveness of RMS's efforts to safeguard confidential information.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- We did not identify instances of a security breach or lost records containing confidential information.

- RMS provides training to RMS employees that covers expectations for handling and consequences for disclosing confidential information.

- Reportable condition related to additional safeguards over confidential information (Finding #2).

FINDING #2

Additional safeguards needed over confidential information.

RMS needs to improve its safeguards for confidential information to minimize the likelihood that confidential data could be accessed by unauthorized personnel.

Agencies send confidential information that can include, but is not limited to, tax returns, social security numbers, and health or other sensitive information to the State Records Center for storage. Our review disclosed that RMS did not:

- Store records based on confidential or sensitive content. We analyzed data corresponding to 145,835 boxes and noted that 38,600 (26%) boxes were recorded as containing confidential information, including federal tax information, social security numbers, personal health information, and personal identifying information (see Exhibit #2). RMS stores all boxes in a similar manner.

- Provide sufficient barriers for active tax information stored at the Records Center. We observed the active tax file storage for Treasury and noted no barriers beyond initial entry into the storage area. IRS Publication 1075 identifies minimum protection standards that establish a uniform method of physically protecting non-electronic forms of federal tax information. Minimum protection standards require two barriers, such as a secured perimeter, security room, employee badges, or secure containers. In addition, IRS Publication 1075 states that information must be containerized in areas where other-than-authorized employees may have access after-hours.

- Sufficiently limit access to the Records Center. We identified 66 (80%) of 83 individuals with access to where all records are stored who were not RMS employees. RMS should restrict Records Center access to only RMS employees. RMS informed us that several individuals are DTMB staff who have access in case of an emergency after-hours.

- Ensure that RMS confidentiality training and agreements were completed on an annual basis. RMS did not have a method of tracking confidentiality training and forms to ensure annual completion. We determined that 100% of RMS employees did not complete an annual confidentiality agreement for calendar year 2016. Also, 3 of the 14 employees did not complete confidentiality agreements during our audit period. RMS provided active file management for Treasury as outlined in an SLA. The agreement stated that any RMS staff assigned to complete these services shall attend the Treasury confidentiality training and also sign an agreement on an annual basis.

RECOMMENDATION

We recommend that RMS improve its safeguards for confidential information to help minimize the likelihood that confidential data could be accessed by unauthorized personnel.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees and will comply with the recommendation. DTMB has improved physical security of the Records Center by reviewing the access list and removing all individuals that do not require access to the Record Center. Individuals that access the warehouse, (e.g. facilities/maintenance/security personnel) will be required to sign in for access. After-hours access will be restricted to a limited number of RMS employees for emergency purposes. Non-RMS employees requiring after-hours access will be escorted. RMS will require and provide confidentiality training to all staff who have badged access to the Records Center.

COMPLIANCE WITH RETENTION AND DISPOSAL SCHEDULES

BACKGROUND

RMS is responsible for establishing retention and disposal schedules* for the official records of each State agency. Schedules are legal documents approved by the initiating agency, RMS, the Archives of Michigan, the Auditor General, the Attorney General, and the State Administrative Board. Approved schedules provide the only legal authority to destroy public records.

Section 18.1285 of the *Michigan Compiled Laws* states that the head of each agency maintaining any record shall cause the records to be listed on a retention and disposal schedule. Legal custody of a record shall be vested in the State agency that created, received, or maintains the record until it is transferred to the State archives or destroyed.

Control Objectives for Information and Related Technology* (COBIT) is a framework adopted by DTMB as a best practice for information technology management and governance.

AUDIT OBJECTIVE

To assess RMS compliance with retention and disposal schedules.

CONCLUSION

Complied, with exceptions.

FACTORS IMPACTING CONCLUSION

- RMS followed approved retention and disposal schedules. Our review of 98 destroyed boxes disclosed that all had met their required retention at the time of disposal.

- We reviewed 258 boxes in Versatile and determined that the calculated retention periods followed approved retention and disposal schedules.

- RMS has implemented a process for agencies to complete self-evaluations of their retention and disposal schedules.

- Reportable conditions related to improving data input to calculate destruction dates (Finding #3) and incorporating electronic records in retention and disposal schedules (Finding #4).

* See glossary at end of report for definition.

FINDING #3

Data input improvements needed to calculate destruction dates.

RMS did not ensure the entry of necessary information into Versatile to calculate destruction dates, resulting in State records that may be retained beyond their approved destruction time period.

We identified 23,728 (7%) of 346,604 boxes at the State Records Center that did not have a calculated destruction date and will not be scheduled for destruction in accordance with approved retention and disposal schedules. Our review disclosed that RMS did not:

- Enter the date of the box content or submission for 11,481 boxes and, therefore, the system will not calculate a destruction date. Of these boxes, 10,829 (94%) should have been destroyed by April 30, 2016.

  The system did not have an edit requiring this information at the time these boxes were submitted to the Records Center.

- Have a process to follow up on 12,247 boxes with an event or indefinite based retention. Event or indefinite based retention boxes require the input of the actual occurrence date in the system in order to calculate a destruction date.

  RMS informed us that it is in the process of eliminating the remaining event and indefinite retentions from existing retention and disposal schedules as the agencies complete their optional self-assessments. The first round of self-assessments began in fiscal year 2013 and were scheduled to be completed by fiscal year 2018. However, RMS does not require the agencies to review and update all of the schedules during the self-assessments.

RECOMMENDATION

We recommend that RMS ensure the entry of necessary information into Versatile to calculate destruction dates.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees and will comply with the recommendation. RMS will work with State agencies to populate the missing box contents dates during each agencies' retention schedule self-evaluation process or by initiating a special project to ensure the entry of necessary information into Versatile to calculate destruction dates.

FINDING #4

Retention and disposal schedules need to incorporate electronic records.

RMS did not ensure that State agencies incorporated records created electronically, including the underlying data that supports electronic records, into retention and disposal schedules. This could result in inconsistent treatment of electronic records and physical records.

Section 18.1284 of the *Michigan Compiled Laws* defines a record as a variety of written, photographed, processed, or recorded mediums "and includes individual letters, words, pictures, sounds, impulses, or symbols, or combination thereof, regardless of physical form or characteristics." Section 18.1287(3)(c) requires DTMB to issue directives that provide for "The submission of proposed retention and disposal schedules to the department of history, arts, and libraries, the auditor general, the attorney general, and the board for review and approval." In addition, COBIT states that agencies should maintain a classification scheme that includes details about data retention and destruction requirements of electronic records. Retention requirements help agencies meet operational, financial reporting, and compliance needs.

As State agencies continue to develop and implement new electronic data systems, RMS should ensure that all records, regardless of their form, are incorporated into retention and disposal schedules.

Although RMS acknowledges the importance of incorporating electronic records into retention and disposal schedules, barriers exist that may mitigate the success of its efforts. Specifically:

- RMS does not have a mandated oversight role in the development of new electronic data systems throughout the State. Such a role would help RMS identify electronic records for inclusion in retention and disposal schedules.

- RMS may need to clarify the definition of a record and its and other State agencies' responsibilities relating to electronic records. The Management and Budget Act (Act 431 of 1984) outlines RMS's roles and responsibilities in the Statewide records retention process. However, many applicable sections of Act 431 have not been revised since 2001. For example, RMS believes that the current definition of a "record" is sufficient and provides a substance-over-form approach in guiding State agencies to incorporate electronic records into retention and disposal schedules. However, our survey of State agency employees with records management responsibilities provided conflicting responses, including employees within the same State agency. RMS should consider an Attorney General Opinion, a DTMB directive, or amendatory legislation to help ensure that State agency employees with records management responsibilities properly incorporate electronic records into retention and disposal schedules.

RECOMMENDATION   We recommend that RMS ensure that State agencies incorporate records created electronically, including the underlying data that supports electronic records, into approved retention and disposal schedules to foster consistency between the handling of electronic and physical records.

AGENCY PRELIMINARY RESPONSE   DTMB provided us with the following response:

DTMB agrees and will comply with the recommendation. RMS is working with DTMB IT leadership to ensure that an evaluation of electronic records is incorporated into the State's systems engineering and development process i.e. "State Unified Information Technology Environment (SUITE)". In addition, RMS will work to provide guidance to State agencies during the development of new electronic records management systems. RMS will work with the Attorney General's office to have the definition of a record clarified.

MONITORING OF CONTRACTS

BACKGROUND RMS is responsible for administering contractual services to ensure proper and efficient destruction of confidential records and for administering master contracts for record reproduction services. During the audit period, RMS contracted with three companies to provide Statewide imaging, microfilm, destruction, and storage services.

AUDIT OBJECTIVE To assess the effectiveness of RMS's monitoring of records management contracts.

CONCLUSION Moderately effective.

FACTORS IMPACTING CONCLUSION

- Treasury conducted a favorable on-site inspection of the confidential destruction contractor and shared the results with RMS. The inspection identified best practices implemented and actions needed. The inspection commended the contractor for its physical and logical security controls and the effectiveness of its controls for safeguarding confidential information.

- RMS maintains frequent communication with the digital imaging contractor.

- Reportable condition related to improvements over contract monitoring (Finding #5).

FINDING #5

Improvements needed over contract monitoring.

RMS did not always monitor its records management contracts to help ensure vendor compliance regarding damaged, lost, or improperly imaged records.

We evaluated RMS's monitoring of contractual obligations for 3 contracts with expenditures totaling $8.1 million during our audit period. For 2 contracts providing imaging, processing, and storage services, making up $7.7 million of the expenditures, RMS did not:

- Ensure that the contractors complied with relevant State of Michigan public acts and standards, including the:

     o   Social Security Number Privacy Act.

     o   Standards for Capturing Digital Images from Paper or Microfilm.

     o   Standards for Capturing Microfilm from Paper.

     o   Standards for Capturing Microfilm from Digital Images.

  The Social Security Number Privacy Act provides guidance for proper safeguarding of individuals' social security numbers. The remaining standards provide guidance for converting official public records to a digital or microfilm format.

- Ensure that the contractors created and provided required production reports. The imaging services contract requires weekly production reports that include job number, department, division, date received, date due, date completed, return date of source documents, number of jobs completed, and job status. Similarly, the processing and storage services contract requires monthly summaries of progress, which outline items such as pending statements of work, status of current jobs in production, accomplishments, problems that must be brought to the attention of RMS, and notification of any significant deviation from the previously agreed upon work plans.

RMS informed us that ongoing communications with the contractors provided sufficient oversight for contract compliance. However, a periodic review of production reports and summaries of progress would provide RMS with a tool to verify the occurrence of contracted activities as well as a basis for evaluating whether on-site contractor monitoring may be warranted.

Alternatively, obtaining a Service Organization Controls* (SOC) 2, type 2 report would provide RMS with independent assurance that contractors were processing, storing, and destroying data in accordance with RMS rules and the terms of their contracts. SOC 2, type 2 reports provide a validation of the contractor's description of the processes' internal control and reports on the suitability of the design and operating effectiveness of those processes. SOC 2, type 2 reports can address any combination of five predefined control principles: security, availability, processing integrity, confidentiality, and privacy. The security, confidentiality, and privacy principles would be most applicable to RMS.

RECOMMENDATION

We recommend that RMS improve the monitoring of its records management contracts.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees and will comply with the recommendation. RMS will improve the monitoring of its records management contracts.

* See glossary at end of report for definition.

SUPPLEMENTAL INFORMATION

RECORDS MANAGEMENT SERVICES
Records Center
Boxes at State Records Center by Agency
As of April 30, 2016

Agency	Number of Boxes
Department of Licensing and Regulatory Affairs	67,561
Michigan Department of Health and Human Services	56,985
Department of Attorney General	33,972
Department of Treasury	28,805
Department of Environmental Quality	25,446
Michigan Department of Transportation	24,364
Department of Insurance and Financial Services	16,952
Court of Appeals	16,915
Supreme Court	13,361
Michigan Department of State Police	10,304
Department of Technology, Management, and Budget	9,209
Department of Military and Veterans Affairs	7,750
Michigan State Housing Development Authority	7,369
Department of State	6,521
Michigan Department of Education	4,361
Department of Natural Resources	3,830
Department of Corrections	3,240
Michigan Economic Development Corporation	2,084
Office of the Auditor General	1,424
Michigan Department of Agriculture and Rural Development	1,394
Department of Civil Rights	1,160
Court of Claims	1,019
Bureau of State Lottery	769
Michigan Strategic Fund	453
Civil Service Commission	418
House of Representatives	385
Senate	362
Senate Fiscal Agency	112
Legislative Council	32
Legislative Retirement	22
Liquor Control Commission	16
Michigan Gaming Control Board	9
Total	346,604

Source: Prepared by the Office of the Auditor General based on unaudited data obtained from RMS's Versatile System.

RECORDS MANAGEMENT SERVICES
Records Center
Review for Confidential Boxes at State Records Center
As of April 30, 2016

Agency	Records Center (Exhibit #1)	Boxes Recorded as Containing Confidential Information
Michigan Department of Health and Human Services	56,985	18,964
Department of Attorney General	33,972	2,643
Department of Treasury	28,805	10,397
Michigan Department of State Police	10,304	409
Department of Military and Veterans Affairs	7,750	5,822
Michigan Department of Education	4,361	296
Department of Corrections	3,240	
Civil Service Commission	418	69
Total	145,835	38,600

Source: Prepared by the Office of the Auditor General based on unaudited data obtained from RMS's Versatile System.

AGENCY DESCRIPTION

Sections 18.1284 - 18.1292 of the *Michigan Compiled Laws* provide for centralized administrative services, including records retention, and state that DTMB shall maintain the records management program for records of the State.

RMS is responsible for:

- Establishing procedures, standards, and techniques for records management activities.

- Operating a records center to house inactive records for State government.

- Developing and approving retention and disposal schedules.

- Providing training to State employees about all aspects of records management.

- Providing centralized microfilming and digital imaging services.

For fiscal years 2014 and 2015, RMS expended $4.7 million and $5.6 million, respectively. As of April 30, 2016, RMS had 14 full-time staff.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE
To examine RMS processes related to services provided to State agencies. 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.

PERIOD
Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2013 through April 30, 2016.

METHODOLOGY
We conducted a preliminary survey of RMS operations to formulate a basis for defining the audit objectives and scope. During our preliminary survey, we:

- Interviewed RMS staff to obtain an understanding of the services provided to State agencies.

- Reviewed applicable laws, policies, procedures, manuals, and guidelines.

- Analyzed information technology systems used by RMS and State agencies.

- Analyzed compliance with records retention and disposal schedules.

- Evaluated RMS's monitoring of contracts.

- Observed the physical security of confidential documents.

OBJECTIVE #1
To assess the effectiveness of RMS's security and access controls over document management systems.

To accomplish this objective, we:

- Reviewed user access for 60 randomly selected users for each of the three main systems (from 1,484 Versatile, 1,194 IRMA, and 1,042 Records Manager users) used by RMS to verify that user access was appropriate.

See glossary at end of report for definition.

- Made inquiries of RMS regarding password policies for each system.

- Reviewed a random sample of 79 service requests to verify that records were sent to a State of Michigan address.

OBJECTIVE #2

To assess the effectiveness of RMS's efforts to safeguard confidential information.

To accomplish this objective, we:

- Analyzed confidential and sensitive information stored at the State Records Center.

- Observed physical security and building access.

- Reviewed annual confidentiality agreements for RMS employees.

- Reviewed individuals with building access to verify that access was appropriate.

OBJECTIVE #3

To assess RMS compliance with retention and disposal schedules.

To accomplish this objective, we:

- Reviewed a random sample of 258 boxes to verify that they were on an approved retention and disposal schedule and the schedule was followed.

- Reviewed a random sample of 98 destroyed boxes to verify that the retention and disposal schedule was followed.

- Made inquiries of RMS regarding the self-evaluation process of records retention and disposal schedules for each agency.

OBJECTIVE #4

To assess the effectiveness of RMS's monitoring of records management contracts.

To accomplish this objective, we:

- Reviewed contract requirements.

- Reviewed communications from contractors.

- Made inquiries of RMS regarding contract monitoring.

CONCLUSIONS   We base our conclusions on our audit efforts and any resulting material conditions* or reportable conditions.

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

AGENCY RESPONSES   Our audit report contains 5 findings and 5 corresponding recommendations. DTMB's preliminary response indicates that RMS agrees 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 an audited agency to develop a plan to comply with the 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.

SUPPLEMENTAL INFORMATION   Our audit report includes supplemental information presented as Exhibits #1 and #2. Our audit was not directed toward expressing a conclusion on this information.

* See glossary at end of report for definition.

GLOSSARY OF ABBREVIATIONS AND TERMS

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.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
Image Repository for Michigan Agencies (IRMA)	A digital image management system administered by RMS for State agencies.
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.
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.
record	Recorded information that is prepared, owned, used, in the possession of, or retained by an agency in the performance of an official function.
Records Manager	A document management system administered by RMS for State agencies.
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.

retention and disposal schedule	A list of records that are created and maintained by a particular office which identifies the period of time that the records need to be retained to satisfy administrative, legal, fiscal, and historical needs.
RMS	Records Management Services.
Service Organization Controls (SOC) report	Designed to help organizations that provide services to user entities build trust and confidence in their delivery processes and controls through a report by an independent certified public accountant (CPA). Each type of SOC report is designed to help service organizations meet specific user needs:

- SOC 1 (Report on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting) - Intended for user entities and the CPAs auditing their financial statements in evaluating the effect of the service organization's controls on the user entities' financial statements.

- SOC 2 (Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy) - Intended for a broad range of users that need information and assurance about a service organization's controls relevant to any combination of the five predefined control principles.

    There are two types of SOC 1 and SOC 2 reports:

    - Type 1 - Reports on the fairness of the service organization's description of controls and the suitability of the design of the controls to achieve the related control objectives included in the description, as of a specified date.

    - Type 2 - Includes the information in a type 1 report and also addresses the operating effectiveness of the controls to achieve the related control objectives included in the description, throughout a specified period.

- SOC 3 (Trust Services Report for a Service Organization) - Intended for those needing assurance about a service organization's controls that affect the security, availability, or processing integrity of the systems a service organization employs to process user entities' information, or the confidentiality or privacy of that information, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 report.

SLA   service level agreement.

State Records Center   A facility that provides off-site storage of inactive records for State
                                 agencies.

Treasury   Department of Treasury.

Versatile   A system that is used to manage the retention and storage of
                                 records at the State Records Center.

OAG

Office of the Auditor General

Independent   Objective   Transparent