Office of the Auditor General
Performance Audit Report

Clarety
Office of Retirement Services
Department of Technology, Management, and Budget

July 2016

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

071-0521-15

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

OAG
Office of the Auditor General

Report Summary

Performance Audit
Clarety
Office of Retirement Services (ORS)
Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0521-15

Released:
July 2016

ORS uses Clarety to electronically obtain wage and contribution information, calculate and pay pension benefits, and maintain the retirement systems' member history and demographic information. These systems include Michigan's Public School Employees' Retirement System (MPSERS), State Employees' Retirement System (MSERS), State Police Retirement System (MSPRS), and Judges' Retirement System (MJRS). As of September 30, 2015, the systems had 518,066 members. DTMB Agency Services is responsible for system development and maintenance, database administration, and data security of Clarety.

Audit Objective			Conclusion
Objective #1: To assess the effectiveness of efforts to ensure the accurate, complete, and timely processing of retirement data by Clarety.			Effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
ORS did not fully establish controls to detect and correct inaccurate retirement option factors, which resulted in pension benefit overpayments totaling $137,200 to one retiree between May 2010 and July 2015 (Finding #1).		X	Agrees

Audit Objective			Conclusion
Objective #2: To assess the effectiveness of security and access controls over Clarety.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
ORS and Agency Services did not fully implement effective security and access controls over the Clarety application and production database to help prevent or detect inappropriate access and modification of data. Access was not timely deactivated after employee departures for 23 of 330 user accounts (Finding #2).		X	Agrees
ORS should require employees to complete annual conflict of interest disclosure statements and review the activity of employees with disclosed conflicts of interest. Annual conflicts of interest statements were not completed by 5 employees with conflicts (Finding #3).		X	Agrees

Audit Objective			Conclusion
Objective #3: To assess the effectiveness of efforts to implement appropriate change controls over Clarety.			Effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Agency Services did not ensure segregation of duties and manage user access for the systems used in the change control process (Finding #4).		X	Agrees

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: www.audgen.michigan.gov

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

OAG
Office of the Auditor General
201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • www.audgen.michigan.gov

Doug A. Ringler, CPA, CIA
Auditor General

July 1, 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 Clarety, Office of Retirement 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

Doug Ringler
Auditor General

TABLE OF CONTENTS

CLARETY

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

ACCURATE, COMPLETE, AND TIMELY PROCESSING OF RETIREMENT DATA

BACKGROUND

During the period October 1, 2013 through July 31, 2015, the Office of Retirement Services (ORS) used Clarety to calculate and pay pension benefits totaling over $9 billion for approximately 274,500 retirees or their beneficiaries in the State's retirement systems. These systems include Michigan's Public School Employees' Retirement System (MPSERS), State Employees' Retirement System (MSERS), State Police Retirement System (MSPRS), and Judges' Retirement System (MJRS):

Retirement System	Number of Members*	Amount of Pension Payments
MPSERS	211,333	$ 6,941,025,700
MSERS	59,597	1,942,181,000
MSPRS	2,993	168,074,100
MJRS	585	33,891,800
Total	274,508	$ 9,085,172,600

AUDIT OBJECTIVE

To assess the effectiveness* of efforts to ensure the accurate, complete, and timely processing of retirement data by Clarety.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- Processes were in place to help ORS identify incomplete processing of interfaces.
- Amount of identified improper payments ($137,200) compared with the $9 billion of total pension benefit payments during the audit period.
- Reportable condition* related to improved accuracy of retirement option factors (Finding #1).

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

FINDING #1

Improvements needed to detect and correct inaccurate retirement option factors.

ORS did not fully establish controls to detect and correct inaccurate retirement option factors, which resulted in pension benefit overpayments totaling $137,200 to one retiree between May 2010 and July 2015. Without sufficient controls in place, ORS could potentially make future inaccurate payments.

Retirement options for MPSERS and MSERS retirees include straight life, 100% survivor, 75% survivor, and 50% survivor. Under the survivor options, the retiree's monthly pension benefit is reduced by an actuarially determined factor based on the combined life expectancies of the retiree and his/her beneficiary. If the beneficiary predeceases the retiree, the monthly pension benefit increases to a straight life pension benefit.

ORS overpaid one retiree $137,200 between May 2010 and July 2015 because of an inaccurate retirement option factor.

Prior to the implementation of Clarety, ORS manually entered retirement option factors into its legacy system. We developed a query and identified 65,318 member records with pension benefits paid during our audit period that were converted from the legacy system into Clarety. We then identified 11 member records for retirees who were predeceased by their beneficiaries. One of these retirees had an inaccurate retirement option factor. Upon the death of the retiree's beneficiary, the retiree's pension benefits were improperly increased because of the inaccurate factor.

ORS designed Clarety to automatically populate retirement option factors for new retirees, which will help prevent the identified error from reoccurring. In addition, ORS indicated that, prior to Clarety, retirement option factors were subject to manual review.

RECOMMENDATION

We recommend that ORS fully establish controls to detect and correct inaccurate retirement option factors.

AGENCY PRELIMINARY RESPONSE

The Department of Technology, Management, and Budget (DTMB) provided us with the following response:

DTMB agrees with the recommendation. ORS will conduct further evaluations of the risk to ensure the appropriate mitigating controls are in place.

SECURITY AND ACCESS CONTROLS OVER CLARETY

BACKGROUND	Security* and access controls* limit or detect inappropriate access, which is important to ensure the availability, confidentiality, and integrity of data.
AUDIT OBJECTIVE	To assess the effectiveness of security and access controls over Clarety.
CONCLUSION	Moderately effective.
FACTORS IMPACTING CONCLUSION	• ORS established extensive operating procedures related to system administration, operations, and security. • Two reportable conditions related to more comprehensive security and access controls (Finding #2) and need to complete and review annual conflict of interest disclosure statements (Finding #3).

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

FINDING #2

More comprehensive security and access controls are needed to prevent and detect inappropriate access.

ORS and Agency Services did not fully implement effective security and access controls over the Clarety application and production database* to help prevent or detect inappropriate access and modification of data.

DTMB Administrative Guide policy 1335 requires State agencies to establish a process to control and document access rights to users. The policy also requires that access be managed, controlled, and periodically reviewed to ensure that user access is based on the principle of least privilege*. In addition, according to DTMB Technical Standard 1340.00.15, database administrators* are required to implement security controls in order to prevent data loss and unauthorized access. Implementation of these controls will provide best practices toward data confidentiality, integrity, and risk management.

We reviewed Clarety's access controls and assessed the configuration* of its production database against Center for Internet Security* benchmarks. Our review disclosed:

User accounts were not timely deactivated after employee departures.

a. ORS had not timely removed access for 23 (7%) of 330 users. Nineteen of the users were students whom ORS no longer employed. The remaining 4 users were individuals who ended their employment with ORS between 1 and 11 months prior to July 31, 2015.

b. ORS did not prevent 32 (10%) of 330 users from having incompatible roles. ORS identified two roles that should not both be granted to a user because they would enable a user to add a new member account and edit retirement information on that account. ORS did not have a control in place to periodically identify and revoke users' access to both roles.

c. ORS did not document the rationale for 3 (7%) of 44 sampled users that had access roles in excess of those approved. ORS indicated that these roles should be removed. Documenting authorization and approvals helps ensure that only appropriate individuals have access to Clarety and that privileges assigned to them are appropriate.

d. Vulnerable security configurations existed on the Clarety database. Because of the confidentiality of database configurations, we summarized the results of our testing for presentation in this finding and provided the detailed results to Agency Services management.

RECOMMENDATION

We recommend that ORS and Agency Services fully implement effective security and access controls over the

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

Clarety application and production database to help prevent or detect inappropriate access and modification of data.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. ORS and its Application Support Team (AST) have both recently updated checklists for four different processes that grant and restrict access for new or transitioning employees. The process enhancements include granting or restricting security access for software, database access, and building access. In addition, these onboarding and offboarding checklists will help prevent inappropriate access and modification of Clarety database data. ORS is also developing training for new supervisors and managers that will include an access requirements review for their staff.

FINDING #3

Need to complete and review annual conflict of interest disclosure statements.

ORS should require employees to complete annual conflict of interest disclosure statements and review employee activity for those with disclosed conflicts of interest. This would help ORS ensure that employees access and modify only member accounts for which they do not have a conflict of interest.

DTMB Administrative Policy 200.04 states that employees must immediately disclose, on a voluntary basis, all personal or financial interests of the employee or the employee's immediate family that are or could become a conflict of interest. At initial hire and as new conflicts arise, employees complete a conflict of interest disclosure form and remit it to DTMB Human Resources rather than ORS. Submitting a separate and more specific annual conflict of interest form to ORS management would allow ORS to monitor the activity of employees with conflicts.

We selected 31 Clarety users and noted that 18 had completed an annual conflict of interest disclosure statement indicating that no conflicts existed. We determined that 4 of the 18 employees did, in fact, have conflicts including spouses and parents with a retirement account. We also determined that 1 of the 13 employees who did not complete a disclosure statement also had a conflict that was not disclosed. These employees did not edit retirement accounts with which they had a conflict during our audit period.

RECOMMENDATION

We recommend that ORS require employees to complete annual conflict of interest disclosure statements and review employee activity for those with disclosed conflicts of interest.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. When requesting staff to complete the annual DTMB conflict of interest disclosure statement, ORS will reinforce DTMB policy and will educate staff on what constitutes a conflict of interest. This annual process will provide clear and consistent direction to staff on when they are required to disclose a conflict of interest. ORS will also create a process to monitor employee activity where a conflict is identified. In addition, ORS currently requires all new employees to sign an ORS conflict of interest form which requires that they are not to work on their own account or any account in which they have a legal or personal relationship.

CHANGE CONTROLS OVER CLARETY

BACKGROUND

Effective change controls* help prevent unauthorized changes to information system resources, such as source code*, and provide reasonable assurance that systems are configured and operating securely and as intended.

AUDIT OBJECTIVE

To assess the effectiveness of efforts to implement appropriate change controls over Clarety.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- ORS established extensive operating procedures related to system development, testing, and quality assurance.
- Sampled Clarety system change requests adhered to ORS's change control process.
- Reportable condition related to the need for segregation of duties* and management of user access for systems used in the change control process (Finding #4).

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

FINDING #4

Effective change control process needed.

Agency Services did not ensure segregation of duties and manage user access for the systems used in the change control process. The lack of controls increased the risk that an unauthorized system change could be processed and go undetected.

Agency Services used Perforce to control access to Clarety source code and Team Track to promote changes to the production environment.

DTMB Administrative Guide policy 1335 requires State agencies to establish a process to control, periodically review, and document the assignment of user access rights. The policy also requires that access be granted to users based on the principle of least privilege and to promote an effective segregation of duties. Our review disclosed:

a. Agency Services did not ensure that access to Team Track promoted an effective segregation of duties.

   Team Track administrator and user roles allow an individual to complete all steps of the change control process, including initiation, development, testing, and moving source code to production. Utilizing change control software with additional privilege-based roles would allow Agency Services to restrict access to users based on job responsibilities and allow for segregation of duties within the change control process.

b. Agency Services had not established a formal policy to periodically review access to Perforce and Team Track.

   Agency Services had not removed access for 5 (8%) of 62 Perforce users and 23 (17%) of 138 Team Track users who were no longer employed or required access to perform their job responsibilities. These users ended their employment between 1 month and 7 years prior to July 31, 2015, the end of our audit period. None of the Perforce user accounts had been used after the employees' departure dates; however, we were unable to determine if the Team Track user accounts were used because Agency Services could not identify when a user last accessed Team Track.

RECOMMENDATION

We recommend that Agency Services ensure segregation of duties and manage user access for the systems used in the change control process.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. The ORS AST upgraded the previous version of Team Track to Serena

Business Manager on June 6, 2016. The Serena Business Manager tool will allow for the creation of more granular privilege-based roles. With this new tool, ORS will also enhance the request/approval workflow to utilize these roles to improve the change control process and provide assurances of "least privilege access." ORS will also determine whether the options available in the Perforce tool will meet these requirements.

In addition, the ORS AST has documented checklists for four different processes that grant and restrict access for new or transitioning employees effective June 2, 2016. These process enhancements now include granting or restricting security access for software, database access, and building access.

DESCRIPTION

ORS acts as the central administrative unit for the State-managed retirement systems. ORS implemented Clarety in 2002 to help accomplish its primary responsibilities, including maintaining accurate member history files, adding new retirees to the pension payrolls, collecting employer and member contributions, and refunding member contributions.

Clarety is a collection of tightly integrated applications for managing and processing the State-managed retirement systems. Components include employer self-service, which is used by reporting units* to report employee wage and contribution data; member self-service, which is used by members to change their demographic information and apply for retirement among other actions; and a customized call center, which is used by the ORS Customer Service Division to address member questions.

Agency Services supports ORS through its mission of ensuring the highest availability of Clarety applications and related systems to end users. Agency Services' primary responsibilities include system development and maintenance, change controls, database administration, and data security.

As of September 30, 2015, there were 518,066 members in MPSERS, MSERS, MSPRS, and MJRS. During the period October 1, 2013 through July 31, 2015, pension benefit payments were made to approximately 274,500 retirees or their beneficiaries totaling over $9 billion.

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

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the information processing and other records related to Clarety. 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 the period October 1, 2013 through July 31, 2015.

METHODOLOGY

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

- Interviewed ORS and Agency Services staff and reviewed system documentation to obtain an understanding of how Clarety collected and processed member data.
- Obtained an understanding of the applications used by ORS to control access to source code and promote changes.
- Reviewed applicable State laws, policies, and procedures related to MPSERS, MSERS, MSPRS, and MJRS.

OBJECTIVE #1

To assess the effectiveness of efforts to ensure the accurate, complete, and timely processing of retirement data by Clarety.

To accomplish this objective, we:

- Performed various data analyses to assess the accuracy and reasonableness of pension benefit payments calculated by Clarety.
- Reviewed various data sets to ensure data reasonableness.

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

- Judgmentally selected interfaces and assessed the design documentation to determine if processes were in place to help ORS identify incomplete or untimely interface processing.

OBJECTIVE #2

To assess the effectiveness of security and access controls over Clarety.

To accomplish this objective, we:

- Reviewed security and access controls over the Clarety application and database.
- Judgmentally selected and evaluated access rights of user accounts with job roles and responsibilities.
- Assessed whether all users are current State employees.

OBJECTIVE #3

To assess the effectiveness of efforts to implement appropriate change controls over Clarety.

To accomplish this objective, we:

- Assessed controls over source code and change management applications, Perforce and Team Track, respectively.
- Judgmentally selected and evaluated access rights of user accounts with access to Perforce and Team Track.
- Randomly selected and evaluated system change requests for adherence to ORS's change control process.
- Compared ORS's change management process with DTMB policy and best practices.
- Randomly selected and evaluated source code changes to determine if the changes related to an authorized system change request.

CONCLUSIONS

We base our conclusions on our audit efforts and the resulting material conditions* and 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.

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

AGENCY RESPONSES

Our audit report contains 4 findings and 4 corresponding recommendations. DTMB's preliminary response indicates that it 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.

GLOSSARY OF ABBREVIATIONS AND TERMS

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
AST	Application Support Team.
Center for Internet Security	A not-for-profit organization that establishes and promotes the use of consensus-based best practice standards to raise the level of security and privacy in information technology systems.
change controls	Controls that ensure that program, system, or infrastructure modifications are properly authorized, tested, documented, and monitored.
configuration	The way a system is set up. Configuration can refer to either hardware or software or the combination of both.
database	A collection of information that is organized so that it can be easily accessed, managed, and updated.
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 operations, performance, integrity, and security of the database.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
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.
member	A retiree or beneficiary currently receiving benefits, a current employee, or a former employee entitled to benefits and not yet receiving benefits.

MJRS	Michigan Judges' Retirement System.
MPSERS	Michigan Public School Employees' Retirement System.
MSERS	Michigan State Employees' Retirement System.
MSPRS	Michigan State Police Retirement System.
ORS	Office of Retirement Services.
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 timing 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.
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.
reporting unit	A public school district, an intermediate school district, a public school academy, a district library, a tax-supported community or junior college, or a university.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.

segregation of duties	Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.
source code	The original form of a computer program before it is converted into a machine-readable code.

This Page Left Intentionally Blank

This Page Left Intentionally Blank


OAG
Office of the Auditor General
Independent
Objective
Transparent