Office of the Auditor General

Performance Audit Report

Michigan Integrated Data Automated System and Michigan Web Account Manager - Selected General and Application Controls

Unemployment Insurance Agency

Department of Labor and Economic Opportunity and Department of Technology, Management, and Budget

May 2022

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

186-0593-21

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.

The auditor general may make investigations pertinent to the conduct of audits.

Article IV, Section 53 of the Michigan Constitution

Performance Audit

Michigan Integrated Data Automated System (MiDAS) and Michigan Web Account Manager (MiWAM) - Selected General and Application Controls

Unemployment Insurance Agency (UIA)
Department of Labor and Economic Opportunity and Department of Technology, Management, and Budget (DTMB)

Report Number:
186-0593-21

Released:
May 2022

MiDAS is an automated information system UIA uses to collect unemployment taxes from employers and pay unemployment insurance benefits to eligible claimants. MiWAM is a system that allows claimants to file and manage their unemployment claims online. UIA, as the business owner, is responsible for ensuring the overall security of MiDAS and MiWAM by defining the systems' security requirements. UIA is also responsible for application controls related to these systems. DTMB, in conjunction with the vendor, FAST Enterprises, is responsible for general controls over the MiDAS database, the MiDAS and MiWAM operating systems, and the State of Michigan (SOM) infrastructure. From March 15, 2020 through June 28, 2021, MiDAS processed $36.5 billion in unemployment claims. UIA has expended $60.8 million on MiDAS development, implementation, and maintenance.

Audit Objective	Conclusion
Objective 1: To assess the effectiveness of UIA's and DTMB's efforts to implement selected security and access controls over MiDAS and MiWAM.	Not effective for UIA Effective for DTMB

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
UIA did not fully implement a variety of controls to safeguard Federal Tax Information. Required background checks were not performed for 36 (80%) of 45 individuals sampled and Internal Revenue Service (IRS) safeguard training was not completed for 27 (60%) of 45 individuals sampled (Finding 1).	X		Agrees

Findings Related to This Audit Objective *(Continued)*	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
For 61 sampled users who had transferred or left State employment, UIA did not disable user accounts timely for 42 (69%) users with MiDAS application access, 30 (49%) users with access to the SOM network, and 41 (67%) users with devices to facilitate remote log-ins (Finding 2).	X		Agrees
UIA did not fully document the purpose and capabilities of groups and functions or identify incompatible functions within the MiDAS application to help ensure the principle of least privilege is followed. For 60 sampled users, UIA did not have complete documentation to support access granted to 15 (25%) of the users sampled (Finding 3).	X		Agrees
Improved compliance with Center for Internet Security (CIS) benchmarks is needed. At least 14 of 42 new or updated CIS benchmark recommendations should be implemented in the State's environment (Finding 4).		X	Agrees
Three (12%) of 25 sampled individuals with MiDAS access did not complete security awareness training (Finding 5).		X	Agrees

Audit Objective	**Conclusion**
Objective 2: To assess the effectiveness of UIA and DTMB's efforts to implement controls over MiDAS and MiWAM interfaces.	Effective

Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
None reported.	Not applicable.		

Audit Objective	**Conclusion**
Objective 3: To assess the effectiveness of UIA and DTMB's efforts to implement change controls over the MiDAS and MiWAM application and data.	Moderately effective

Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
UIA did not properly document the authorization to initiate 13 (39%) system changes sampled and did not maintain documentation of post-implementation testing for 8 (24%) changes sampled (Finding 6).		X	Agrees

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

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

This Page Left Intentionally Blank

OAG

Office of the Auditor General

Doug A. Ringler, CPA, CIA
Auditor General

201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • audgen.michigan.gov

May 17, 2022

Ms. Susan R. Corbin, Director
Department of Labor and Economic Opportunity
300 North Washington Square
Lansing, Michigan

Ms. Julia Dale, Director
Unemployment Insurance Agency
Cadillac Place
Detroit, Michigan

Ms. Michelle Lange, Acting Director
Department of Technology, Management, and Budget
and
Ms. Laura Clark, Chief Information Officer
Department of Technology, Management, and Budget
Elliott-Larsen Building
Lansing, Michigan

Dear Ms. Corbin, Ms. Dale, Ms. Lange, and Ms. Clark:

This is our performance audit report on the Michigan Integrated Data Automated System and Michigan Web Account Manager - Selected General and Application Controls, Unemployment Insurance Agency, Department of Labor and Economic Opportunity and Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agencies 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 to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, 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

This Page Left Intentionally Blank

TABLE OF CONTENTS

MICHIGAN INTEGRATED DATA AUTOMATED SYSTEM AND MICHIGAN WEB ACCOUNT MANAGER - SELECTED GENERAL AND APPLICATION CONTROLS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

SELECTED SECURITY AND ACCESS CONTROLS

BACKGROUND

Security* controls are the management, operational, and technical controls designed to protect the availability*, confidentiality*, and integrity* of a system and its information.

Access controls* limit or detect inappropriate access to computer resources, thereby protecting the resources from unauthorized modification, loss, and disclosure. For access controls to be effective, they should be properly authorized, implemented, and maintained.

As of August 17, 2021, 3,740 users had access to the Michigan Integrated Data Automated System* (MiDAS).

AUDIT OBJECTIVE

To assess the effectiveness* of Unemployment Insurance Agency's (UIA's) and Department of Technology, Management, and Budget's (DTMB's) efforts to implement selected security and access controls over MiDAS and the Michigan Web Account Manager* (MiWAM).

CONCLUSION

Not effective for UIA.

Effective for DTMB.

FACTORS IMPACTING CONCLUSION

- Three material conditions* related to establishing and implementing effective application access controls (Findings 1 through 3).
- Two reportable conditions* related to implementing effective security configuration controls and ensuring MiDAS application users complete security awareness training (Findings 4 and 5).
- MiDAS and MiWAM system security parameters were substantially implemented, or in the process of being implemented, in accordance with State and industry best practices.
- DTMB established and implemented some policies, standards, and procedures related to security of the Windows server environment.
- DTMB implemented security configurations of Microsoft SQL databases in accordance with State policy and adopted industry best practices.

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

FINDING 1

Improved safeguards over FTI needed.

UIA did not always conduct required safeguards to protect federal tax information* (FTI). Safeguarding FTI is critically important to continuously protect taxpayer confidentiality as required by Internal Revenue Code (IRC) Section 6103.

Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies*, states agencies legally receiving FTI from the IRS or other sources must have adequate programs in place to protect the data. Furthermore, as agencies procure the services of contractors, it becomes equally important for contractors to protect FTI from unauthorized access, use, and disclosure.

Publication 1075 also states, prior to granting access to FTI and periodically thereafter, employees must receive disclosure awareness training and the agency must complete a suitability background investigation. Background investigations for any individual granted access to FTI must include, at a minimum, Federal Bureau of Investigation fingerprinting, a local law enforcement check, and a citizenship/residency validation.

We randomly sampled 45 of the 330 individuals who had the ability to, at a minimum, view FTI. Our review disclosed UIA did not:

Required background checks and IRS training were not performed for 80% and 60% of users sampled, respectively.

a. Perform required background checks for 36 (80%) individuals. Of these 36 individuals, 5 were UIA employees and 31 were DTMB employees or contractors.

b. Ensure IRS safeguard training completion by 27 (60%) individuals. Of these 27 individuals, 5 were UIA employees and 22 were DTMB employees or contractors.

c. Sufficiently track individuals with access to view FTI. Of the 45 individuals sampled, 16 (36%) were not included on UIA's internal tracking sheet. UIA utilizes this sheet to ensure users requiring access to FTI for their job duties have completed the required safeguard measures. Of the 16 individuals, 5 were UIA employees and 11 were DTMB employees or contractors.

d. Sufficiently monitor logs generated at the MiDAS application level to ensure individuals viewing FTI were properly authorized. State of Michigan (SOM) Technical Standard 1340.00.040.01 requires the information system owner to ensure information system audit records are reviewed and analyzed at least weekly. UIA indicated it began reviewing the logs monthly, as of approximately March 2020.

UIA informed us it had not identified the complete population of UIA, DTMB, and contracted employees with access to FTI for whom to perform the required background check and IRS training.

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

We consider this finding to be a material condition because of the legal requirements for safeguarding FTI, the sensitive nature of FTI, and the collective number of deficiencies identified.

RECOMMENDATION

We recommend that UIA conduct required safeguards to protect FTI.

AGENCY PRELIMINARY RESPONSE

UIA provided us with the following response:

UIA agrees that the required safeguards should be conducted to protect FTI. In second quarter 2022, UIA will meet with DTMB and all contractors to identify all individuals who have access to FTI.

With respect to the specific elements of this finding, we have the following responses:

a. *UIA agrees. On April 12, 2022, UIA issued the Criminal History Check and Fingerprinting Policy which requires criminal history checks on all users who have access to confidential information in UIA's possession. The criminal background checks will be conducted in 2022 on all UIA staff, DTMB staff, and contractors who have access to personally identifiable information and/or FTI.*

b. *UIA agrees. After identification of all users who have access to FTI, IRS safeguard training will be completed within 60 days. The Internal Controls Division recently hired a new analyst who will track all individuals who have access to view FTI and will document training course completion dates.*

c. *UIA agrees. The internal controls analyst will compare weekly the UIA internal tracking log against access logs of individuals who viewed FTI.*

d. *UIA agrees. The internal controls analyst will begin monitoring logs and auditing system records weekly.*

FINDING 2

Timely removal of user access needed.

UIA should establish a process to ensure the timely removal of MiDAS user access rights. Delayed removal can result in unauthorized access to MiDAS, allowing users the ability to view confidential information, change or update claim information, and process inappropriate claims.

SOM Technical Standard 1340.00.020.01 requires data custodians be notified when accounts are no longer required, terminated, or transferred or when individual information system usage privileges change. In this case, the information system owner, UIA, must notify the data custodian, DTMB, within 24 hours of a user's job termination or transfer or immediately if required based on system data classification or after an unfriendly separation. Data custodians must remove access immediately or within 48 hours depending on data classification.

To access MiDAS, a user requires active access to the SOM network, MiDAS application, as well as access to the virtual private network through the use of an RSA* token while working off site.

We sampled 61 users (54 contractors and 7 UIA employees) whose MiDAS access was terminated between January 2021 and August 2021 to determine whether UIA and DTMB had disabled access timely. We noted:

a. UIA did not disable MiDAS application access within 72 hours of employee departure or transfer for 42 (69%) of the 61 users sampled.

b. UIA did not request DTMB to terminate SOM network access within 24 hours of employee departure or transfer for 30 (49%) of the 61 users sampled.

c. UIA did not request DTMB to terminate RSA token access within 24 hours of employee departure or transfer for 41 (67%) of the 61 users sampled.

d. UIA did not ensure any of the three credentials were disabled for 17 (28%) of the 61 users sampled. Twelve of these individuals had access ranging from 4 to 39 days beyond their departure date, with an average of 9 days. These 17 users retained access at all three levels which allowed them inappropriate access to MiDAS.

MiDAS application access, SOM network access, and RSA token access were not disabled for 69%, 49%, and 67% of users tested, respectively.

DTMB indicated that controls are in place to deactivate a user's SOM network access after an account is inactive for 61 days.

UIA did not have a process in place to offboard users from contracted groups in a timely manner. This issue was compounded by the COVID-19* pandemic, which caused UIA to substantially increase the number of contracted employees.

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

We noted a similar condition in our March 2022 performance audit* of Personnel Management Processes During the COVID-19 Pandemic, Unemployment Insurance Agency, Department of Labor and Economic Opportunity (186-0310-21). In response to that finding, UIA indicated it agreed with the recommendation and reviewed and improved the removal process by increasing the frequency to daily offboarding of contract staff who have left. Also, UIA indicated it will implement a quality control process for frontline managers and the Internal Controls Division to review timely removal of system access for all contract workers and UIA employees.

We consider this finding to be a material condition because of the importance of timely removal of user access in securing MiDAS and the collective number of deficiencies identified.

RECOMMENDATION

We recommend that UIA establish a process to ensure the timely removal of user access rights.

AGENCY PRELIMINARY RESPONSE

UIA provided us with the following response:

UIA agrees that user access rights should be removed timely. UIA is currently formalizing the quality control process requiring management to timely terminate MiDAS, SOM network and RSA token access to ensure we are in compliance with SOM Technical Standard 1340.00.020.01. In addition, the Internal Controls Division will audit weekly the timely removal of MiDAS user access rights.

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

FINDING 3

Effective access controls not fully established and implemented.

UIA did not fully establish and implement effective application access controls over MiDAS, thereby increasing the risk of unauthorized access, use, and modification of unemployment insurance data.

SOM Technical Standard 1340.00.020.01 defines the security control baselines for access to information systems. The Standard requires State agencies to establish a process to control and document the assignment of access rights based on current job responsibilities and the principle of least privilege*. The Standard also requires monitoring user activity, reviewing access rights annually for appropriateness, disabling accounts inactive for more than 60 days, and disabling or deleting user accounts in a timely manner.

Also, the Federal Information System Controls Audit Manual* (FISCAM) recommends listings of authorized users and their specific access needs and any modifications be approved by an appropriate senior manager and directly communicated in writing by the resource owner to the security management function. In addition, FISCAM recommends an entitywide policy outlining the responsibilities of groups and related individuals pertaining to incompatible activities be documented, communicated, and enforced.

Our review of MiDAS access controls disclosed:

a. UIA did not fully establish a formal process to grant MiDAS application access to align with users' job responsibilities. UIA did not:

   (1) Consistently list all groups or functions on user access request forms nor did UIA always have complete supporting documentation for access granted to users.

   MiDAS user access rights are based on the groups and functions granted to the user. A group consists of a series of functions. A user can be assigned to multiple groups or a combination of groups and functions. Functions allow a user to perform actions such as view, input, and edit data; process transactions; and approve payments.

   We judgmentally sampled 60 of 3,740 active MiDAS users as of August 17, 2021 and reviewed their access authorization forms to determine whether access was appropriately authorized. UIA did not specify the groups and functions to which the users should be assigned for 5 (8%) of the 60 users. Identifying specific access needs reduces the risk of misunderstanding between UIA managers who request the access and DTMB who

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

Complete supporting documentation was not available for access granted to 25% of users tested. Also, 3% of users had rights unnecessary for their job duties.

grants it. Also, UIA did not have complete supporting documentation for the access granted to 15 (25%) of the 60 users.

(2) Document group and function capabilities to ensure MiDAS users are granted appropriate access rights necessary to perform their jobs.

UIA informed us its program managers primarily relied on UIA's Agency Services Division to advise them which groups and functions to assign to new users within MiDAS. Guidance fully describing the capabilities of groups and functions was not established for staff, security administers, program managers, and supervisors to use when requesting groups and functions for a new user or to change an existing user's access.

(3) Identify incompatible functions or excessive access rights to ensure effective segregation of duties* and access based on the principle of least privilege.

We judgmentally sampled 60 of 3,740 active users as of August 17, 2021 to determine whether selected access rights assigned to the users were appropriate. Two (3%) of the users had FTI access rights that were unnecessary for their job duties and position in UIA.

Identifying incompatible functions is a key control in effective segregation of duties. Conversely, inadequate segregation of duties increases the risk erroneous or fraudulent transactions could be processed. UIA should limit access rights to those necessary for users to perform their day-to-day tasks to reduce the potential of inappropriate use of MiDAS.

b. UIA did not always perform effective user account management. UIA did not:

(1) Disable user accounts of departed contractors.

User accounts of departed contractors were not disabled for 5% of all active contractor accounts.

We reviewed all 2,533 active MiDAS contractor accounts as of August 17, 2021 and determined 132 (5%) were associated with a contractor no longer employed by the State, and therefore, no longer required access. To prevent misuse, UIA should disable user accounts on a timely basis.

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

After bringing this matter to management's attention, UIA disabled the 132 departed contractor accounts.

(2) Establish a timely process to consistently ensure accounts were inactivated after 60 days of inactivity.

MiDAS automatically runs a job on the last business day of each month to create a security case for each MiDAS user account inactive for 60 days or more. Each security case is manually reviewed by UIA to determine whether the user's account should be disabled. If the account should be disabled for inactivity, UIA approves the case and submits it to DTMB to disable the account.

Accounts inactive for 59 days, as of the date the job runs, would not be identified until the job runs the following month. Therefore, it is possible a user account could be inactive up to 89 days before the account is disabled. Disabling inactive accounts timely reduces the risk of inappropriate activity in MiDAS.

(3) Conduct annual recertifications of user access rights.

User access rights should be periodically recertified to ensure privileges granted to each user are still appropriate for the user's job responsibilities.

UIA informed us it did not maintain effective access controls because of the COVID-19 pandemic-related workload and the need to onboard an unprecedented number of new staff in a very short time period.

We noted a similar condition in our February 2016 performance audit of Michigan Integrated Data Automated System (MiDAS), Unemployment Insurance Agency, Department of Talent and Economic Development, and Department of Technology, Management, and Budget (641-0593-15). In response to that audit, UIA indicated it agreed with the recommendation and implemented controls to find and disable inactive accounts and conduct periodic review of access activity.

We consider this finding to be a material condition because of (1) the risk of fraudulent transactions being processed, (2) the potential for inappropriate use of MiDAS, and (3) the importance of access controls in MiDAS, which contains sensitive and confidential information such as personally identifiable information and FTI.

RECOMMENDATION

We recommend that UIA fully establish and implement effective application access controls over MiDAS.

AGENCY PRELIMINARY RESPONSE

UIA provided us with the following response:

UIA agrees that effective application controls over MiDAS should be fully established and implemented.

With respect to the specific elements of this finding, we have the following responses:

a. UIA agrees that MiDAS application access should align with the user's job responsibilities. As part of the FAST Core 21 upgrade with an implementation date of July 5, 2022, MiDAS user access rights will be granted on an individual basis based on their specific job requirements and the principle of least privilege will be followed. During this process, incompatible functions and excessive access rights will be identified and addressed appropriately to ensure effective segregation of duties.

b. *UIA agrees that user accounts should be effectively managed. UIA is currently formalizing the process requiring management to timely terminate MiDAS, SOM network, and RSA token access to ensure compliance with SOM Technical Standard 1340.00.020.01. In addition, the Internal Controls Division will audit monthly the timely removal of MiDAS user access rights, including those of contractors. Additionally, the MiDAS job run will now be ran on MiDAS user accounts that have been inactive for 30 days. Finally, UIA will require annual recertification of user access rights beginning in 2023, since user rights are being reviewed in 2022 during the Core 21 upgrade.*

FINDING 4

Improvements needed to ensure compliance with CIS benchmarks.

DTMB did not fully develop and document processes to review Center for Internet Security* (CIS) benchmarks to identify recommendations appropriate to the State's environment and monitor ongoing compliance with the recommendations. As a result, DTMB could not readily verify MiDAS and MiWAM servers conform with security best practices.

SOM Technical Standard 1345.00.13 requires DTMB to ensure servers are tailored from components of various best practices and SOM technical standards, including CIS. Also, DTMB Technical Standard 2019.09.15.01, *Technical Services Server Operating System Configuration Standard*, requires DTMB to maintain operating systems that conform with CIS benchmarks.

Our review of DTMB's process for securing the MiDAS and MiWAM servers according to CIS benchmark recommendations disclosed:

a. DTMB did not periodically review new and updated CIS benchmark security recommendations to determine whether to adopt the recommendations in the MiDAS and MiWAM server environments.

   DTMB configured MiDAS and MiWAM servers to version 1.0.0 of the CIS benchmarks for Windows Server 2016. CIS published version 1.2.0 in May 2020. We compared the two versions and identified 42 new or updated recommendations had not been implemented on the MiDAS and MiWAM servers. DTMB evaluated the 42 recommendations we identified and determined:

   (1) 14 recommendations should be implemented.

   (2) 14 recommendations could not be implemented in the MiDAS and MiWAM server environment.

   (3) 1 recommendation needs to be evaluated further by DTMB.

   (4) 13 recommendations were already configured in the servers.

   Without reviewing and implementing updated CIS benchmarks, MiDAS and MiWAM servers may be at risk.

b. DTMB's tool to test and monitor server compliance with CIS benchmarks did not test for all CIS version 1.0.0 benchmark recommendations.

   DTMB uses a third-party tool to test and monitor for compliance with the adopted CIS benchmark

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

recommendations. However, the tool did not test 5 of the 245 adopted recommendations. As a result, DTMB cannot readily ensure server compliance with CIS benchmark recommendations.

DTMB informed us limitations with the tool were the reason why 2 of the 5 recommendations were not tested.

c. DTMB did not formally document its business case and management approval for all CIS benchmark recommendations it did not adopt.

   DTMB developed a process to assess and test CIS benchmarks before adopting them in the MiDAS and MiWAM server environment, including a documented business case for recommendations not adopted. Our review of the CIS benchmarks not adopted noted DTMB did not document the business cases and appropriate management approvals for 6 recommendations. Without formal documentation, DTMB cannot ensure recommendations not adopted were properly evaluated for the MiDAS and MiWAM server environment.

   After bringing this to management's attention, DTMB formally documented the business cases for 4 of the 6 recommendations not adopted. DTMB informed us the remaining 2 recommendations could not be implemented for the MiDAS and MiWAM database servers as they would prevent DTMB from performing backups of the servers.

We noted a similar condition in our February 2016 performance audit of Michigan Integrated Data Automated System (MiDAS), Unemployment Insurance Agency, Department of Talent and Economic Development and Department of Technology, Management, and Budget (641-0593-15, Finding 2, part a). In response to that audit, DTMB indicated it agreed with the recommendation and would implement an automated configuration management tool. DTMB has complied with parts b. through d. of Finding 2. It implemented an automated configuration management tool and developed a list of CIS benchmarks to support the Windows configuration management process.

RECOMMENDATION

We recommend that DTMB fully develop and document processes to review CIS benchmarks to identify recommendations appropriate to the State's environments and monitor ongoing compliance with the recommendations.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the need to enhance, develop and document processes to review and tailor CIS benchmarks appropriate to the

State's environment; and to document processes for monitoring on-going compliance with the tailored benchmarks. As such, DTMB:

- *Conducted an initial workshop to review existing processes and identify additional processes for development.*

- *Is reviewing the tailored benchmarks currently in use in the State's environment for appropriateness. DTMB will document approval of the tailored benchmarks.*

- *Will document and enhance standards and procedures as necessary.*

FINDING 5

Improvements needed to ensure completion of security awareness training.

UIA did not ensure all individuals with access to MiDAS completed security awareness training. Lack of training on the responsibilities for safeguarding data increases the likelihood of inappropriate disclosure of sensitive or confidential data.

Section 421.11 of the *Michigan Compiled Laws* states that MiDAS data, including names, social security numbers, and wages, is confidential and shall not be disclosed or open to public investigation. SOM Technical Standard 1340.00.030.01 requires the agency information system owner to provide basic security awareness training to information system users and contractors. Also, the UIA Data Governance Policy states that staff must complete all compliance training modules within the first week of hire and complete refresher training modules annually.

We randomly sampled 25 individuals with active MiDAS access as of August 17, 2021. Three (12%) of the 25 did not complete annual security training and sign the data governance acknowledgment form as required by UIA Data Governance Policy and SOM technical standards. Of the three individuals:

- One DTMB contractor did not complete the security training, because UIA did not require DTMB contractors to do so. UIA did not obtain an exemption allowing for the deviation from SOM Technical Standard 1340.00.030.01.

- UIA did not maintain documentation of 2 UIA contractors' signed acknowledgment forms. UIA informed us it could not locate these forms.

We noted a similar condition in our February 2016 performance audit of Michigan Integrated Data Automated System (MiDAS), Unemployment Insurance Agency, Department of Talent and Economic Development and Department of Technology, Management, and Budget (641-0593-15). In response to that audit, UIA indicated it agreed with the recommendation and implemented a systematic training process.

RECOMMENDATION

We recommend that UIA ensure all individuals with access to MiDAS complete security awareness training.

AGENCY PRELIMINARY RESPONSE

UIA provided us with the following response:

UIA agrees that all individuals with access to MiDAS should complete security awareness training. UIA will conduct criminal background checks in 2022 on all UIA staff, DTMB staff, and contractors who have access to confidential UI data. In addition, UIA will also require and conduct security awareness training these same individuals. The recently hired Internal Controls Division analyst who tracks and logs all individuals with FTI access will also track and log all compliance and security awareness trainings.

INTERFACE CONTROLS

BACKGROUND

Interface controls* ensure the accurate, complete, and timely processing of data between systems. MiDAS has more than 100 inbound and outbound interfaces, including:

- IRS: Provides the 1099-MISC extract file to State unemployment agencies for the purpose of tax administration.
- Employer Filed Claims: Receives unemployment claims filed by employers on behalf of laid-off employees.
- Benefits Paper Check: Sends unemployment checks to the Consolidated Print Center for printing and mailing.

Ensuring MiDAS contains accurate, complete, and timely data is the responsibility of UIA, in conjunction with DTMB.

AUDIT OBJECTIVE

To assess the effectiveness of UIA and DTMB's efforts to implement controls over MiDAS and MiWAM interfaces.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- MiDAS interface design documentation generally complied with industry best practices.
- For 100% of interfaces sampled, the job was completed and the interface files were retrieved and loaded into the database tables.
- DTMB implemented error handling procedures to ensure processing errors were corrected in a timely manner.

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

CHANGE CONTROLS

BACKGROUND

Changes to MiDAS and MiWAM are typically initiated when UIA authorizes a needed modification. DTMB or the third-party vendor constructs the change in a development environment before moving to a test environment where the change undergoes various quality assurance and user acceptance testing. Upon completion of testing, UIA authorizes DTMB to move the change into the production environment. Then UIA conducts a post-implementation review to verify the change meets user expectations.

MiDAS and MiWAM changes generally consist of system upgrades, implementation of new programs, and correction of programming errors. Beginning in October 2019 and throughout the COVID-19 pandemic, 653 (22%) of the 2,982 changes implemented to MiDAS and MiWAM were related to new COVID-19 pandemic unemployment assistance programs.

All SOM agencies are required to follow the Systems Engineering Methodology* (SEM) for IT projects. SEM is a component of the State Unified Information Technology Environment* (SUITE), which provides guidance for project management activities and quality assurance practices and procedures. SEM also aids in status tracking, management control, and documentation efforts of a project.

AUDIT OBJECTIVE

To assess the effectiveness of UIA and DTMB's efforts to implement change controls* over the MiDAS and MiWAM application and data.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- UIA and DTMB appropriately utilized the Fast Code Repository to centrally store documentation of the initiation, construction, testing, implementation, and closeout phases of the change management process.

- UIA and DTMB appropriately implemented some controls over system changes in accordance with State policies, standards, and procedures.

- One reportable condition related to implementing more effective change controls (Finding 6).

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

FINDING 6

More effective change controls needed.

UIA, in conjunction with DTMB, did not fully implement effective change controls over the MiDAS and MiWAM applications and data to ensure all system changes were authorized and operating as intended before being implemented.

The State of Michigan Administrative Guide to State Government policy 1355 establishes project management best practices as a component of SUITE. SOM Technical Procedure 1340.00.060.04 and SOM Technical Standard 1340.00.060.04.01 establish the methods required for change management.

We judgmentally and randomly sampled 33 changes, referred to as Solution Quality Requests (SQRs), UIA and DTMB made to MiDAS and MiWAM between October 2019 and June 2021. Our review disclosed:

a. UIA did not document the various levels of review and approval of the business requirements on the request for automation services form, form 6431, for 13 (39%) of the 33 SQRs reviewed.
   SOM Technical Standard 1340.00.060.04.01 requires the business owner* to document and approve the business requirements prior to development.

b. UIA did not document post-implementation testing for 8 (24%) of the 33 SQRs reviewed.
   SOM Technical Standard 1340.00.060.04.01 requires the business owner to perform post-implementation validation of system changes to ensure the changes were applied and functioning as intended.

c. UIA, in conjunction with DTMB and its software vendor, should improve its change control processes to meet SUITE SEM requirements. Specifically, UIA needs to ensure:

   (1) Formalized change management policies and procedures are documented and implemented at the application level to ensure an effective process.

       FISCAM states such procedures should cover employee roles and responsibilities, change control and system documentation requirements, and the establishment of a decision-making structure.

   (2) Documentation of DTMB's and the software vendor's system integration testing is maintained. This will ensure new software code will not impact the existing MiDAS and MiWAM functionalities and the updated functionalities meet the design of the system.

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

SOM Technical Standard 1340.00.060.04.01 requires the technical development team to perform system integration testing. The SUITE System Maintenance Guidebook requires integration testing in which the proper interaction between system components is verified.

(3) User acceptance testing (UAT) is performed at sufficient and appropriate levels to verify system changes are working as intended and reduce any unintended consequences prior to implementation into production.

SOM Technical Procedure 1340.00.060.04 requires the business owner to perform UAT to ensure system changes meet the documented requirements by testing against documented test plans.

UIA informed us the formal change management process was not strictly followed because of deadline time constraints and the vast number of changes required to implement the Coronavirus Aid, Relief, and Economic Security (CARES) Act programs.

RECOMMENDATION

We recommend that UIA, in conjunction with DTMB, fully implement effective change controls over the MiDAS and MiWAM applications and data to ensure all system changes are authorized and operating as intended before implementation.

AGENCY PRELIMINARY RESPONSE

UIA provided us with the following response:

UIA agrees that effective change controls should be fully implemented over the MiDAS and MiWAM applications and data to ensure all system changes are authorized and operating as intended before implementation. UIA is the process of developing a change management procedure to address these findings. With respect to the specific elements of this finding, we have the following responses:

a. *UIA agrees. UIA is in the process of developing a change management procedure that will require and maintain documentation of approval for business changes. A request for automation service ticket or other approval documentation must be fully completed with all necessary sign-offs before Agency Services will process the request.*

b. *UIA agrees. UIA is in the process of developing a change management procedure that will require documentation be maintained for all post-implementation verification.*

c. *UIA agrees. UIA is in the process of developing a change management procedure that will incorporate appropriate*

SUITE SEM requirements to minimize the likelihood new software code will materially impact the existing MiDAS and MiWAM functionalities.

SYSTEM DESCRIPTION

MiDAS is an automated information system used by UIA to collect unemployment taxes from employers and pay unemployment insurance benefits to eligible claimants. MiDAS was fully implemented in October 2013. The goals of MiDAS included improved customer service, increased data accuracy, improved data security and privacy, reduced operating costs, increased automation, and improved integration of UIA functions. UIA has expended $60.8 million on development, implementation, and maintenance of MiDAS. From March 15, 2020 through June 28, 2021, MiDAS processed $36.5 billion in unemployment claims.

MiWAM is a system that allows claimants to file and manage their unemployment claims online. Claimants can update their personal information, check their claim balance and benefit payment history, submit questions, and file protests or appeals within MiWAM, among other functionalities.

UIA, as the business owner, is responsible for ensuring the overall security of MiDAS and MiWAM by defining the systems' security requirements.

UIA is also responsible for application controls such as user access and input, processing, and output controls related to collecting taxes and processing unemployment claims within MiDAS to facilitate Michigan's unemployment insurance program and deliver unemployment services to claimants. UIA shares responsibility with DTMB for change management and interface controls.

DTMB, in conjunction with the vendor, FAST Enterprises, is responsible for general controls over the MiDAS database, the MiWAM and MiDAS operating systems, and the SOM infrastructure. In addition, FAST Enterprises is responsible for the development of MiDAS and MiWAM and assists with the maintenance and security of the systems.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine MiDAS and MiWAM records and processes related to security and access controls, interface controls, and change 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit did not include a review of MiWAM business process application-level controls, including those related to authorization controls and data processing controls.

As part of the audit, we considered the five components of internal control* (control environment, risk assessment, control activities, information and communication, and monitoring activities) relative to the audit objectives and determined all components were significant.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2019 through September 30, 2021.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of UIA and DTMB's processes and internal control to establish our audit objectives, scope, and methodology. During our preliminary survey, we:

- Interviewed UIA and DTMB management and staff to obtain an understanding of MiDAS and MiWAM.

- Reviewed UIA and DTMB policies and procedures related to MiDAS and MiWAM security.

- Reviewed system documentation, including the contract for MiDAS development, the implementation methodology, and system configurations.

- Obtained an understanding of UIA and DTMB's key processes, systems, and internal control significant to the potential audit objectives.

- Obtained an understanding of UIA and DTMB's processes for:

  - Granting and monitoring user access to MiDAS.

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

  - Managing database and operating system configurations, access, patching, vulnerability management, and monitoring.

  - Implementing firewall controls, change controls, and interface controls for MiDAS and MiWAM.

  - Providing security awareness training for MiDAS users.

OBJECTIVE 1

To assess the effectiveness of UIA's and DTMB's efforts to implement selected security and access controls over MiDAS and MiWAM.

To accomplish this objective, we:

- Identified MiDAS users and tested for:

  - All active accounts assigned to users no longer employed by the State.

  - Active accounts assigned to contractors no longer working for the State.

- Evaluated the design of UIA's process to inactivate users that had not logged in to MiDAS in at least 60 days.

- Evaluated the design of UIA's process to monitor and recertify users.

- Randomly sampled 60 of 3,740 active users as of August 2021 to determine whether UIA:

  - Maintained user access forms and security agreements and approved the access forms.

  - Granted access to the MiDAS profiles requested on the access forms.

- Interviewed UIA management to obtain an understanding of MiDAS segregation of duties.

- Tested the end-user account security configurations of MiDAS and MiWAM against SOM policy and industry best practices.

- Judgmentally and randomly sampled 1 MiDAS server out of 3 and 1 MiWAM server out of 2 as of June 2021 and:

  - Tested the appropriateness of user access to selected databases.

    - Compared database configurations with adopted industry best practices and SOM technical standards.

    - Reviewed database vulnerability reports to assess whether outstanding and mitigated vulnerabilities complied with SOM technical standards.

    - Identified current patch levels on Microsoft SQL databases and evaluated against vendor recommendations.

    - Validated audit logs were enabled and captured information as required by SOM technical standards.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. For our judgmental samples, we could not project the results to the respective populations.

OBJECTIVE 2

To assess the effectiveness of UIA and DTMB's efforts to implement controls over MiDAS and MiWAM interfaces.

To accomplish this objective, we:

- Obtained an understanding of the population of interfaces with MiDAS and MiWAM.

- Reviewed interface definition documents for compliance with industry best practices.

- Judgmentally and randomly sampled 10 of 94 system interfaces in place as of August 10, 2021 and validated the files were retrieved and loaded onto the database tables for randomly selected dates.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. For our judgmental samples, we could not project the results to the respective populations.

OBJECTIVE 3

To assess the effectiveness of UIA and DTMB's efforts to implement change controls over the MiDAS and MiWAM application and data.

To accomplish this objective, we:

- Compared UIA and DTMB's change management process with the State's policies, procedures, and best practices.

- Reviewed a judgmental and random sample of 33 of 2,982 system changes implemented in MiDAS or MiWAM from October 1, 2019 through June 22, 2021 for compliance with the State's change management policies, procedures, and best practices.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. For our judgmental samples, we could not project the results to the respective populations.

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 6 findings and 6 corresponding recommendations. UIA's and DTMB's preliminary responses indicate that they agree with all of the recommendations.

The agency preliminary response following each recommendation in our report was taken from the agencies' written comments and oral discussion at the end of our 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 to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, 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.

PRIOR AUDIT FOLLOW-UP

Following is the status of the reported findings from our February 2016 performance audit of the Michigan Integrated Data Automated System (MiDAS), Unemployment Insurance Agency, Department of Talent and Economic Development and Department of Technology, Management, and Budget (641-0593-15):

Prior Audit Finding Number	Topic Area	Current Status	Current Finding Number
1	MiDAS security management program needs to be enhanced.	Rewritten*	5
2	Improvements needed to operating system security and access controls.	Rewritten	4
3	Access to the MiDAS application should be better controlled.	Rewritten	3
4	Security improvements needed to the MiDAS database containing confidential claimant information.	Complied	Not applicable
5	Automated controls needed to identify claimants who have not submitted evidence of work searches.	Not in scope of this audit.	
6	Additional data analysis will help detect payments needing further review.	Not in scope of this audit.	
7	Changes needed to improve the appeals process.	Not in scope of this audit.	
8	Opportunities exist for additional automation using MiDAS.	Not in scope of this audit.	

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

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.

availability Timely and reliable access to data and information systems.

business owner The person responsible for administration of systems. A business owner is usually the owner of the primary business functions served by the application or the application's largest stakeholder.

Center for Internet Security (CIS) 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 IT systems.

change controls Controls that ensure program, system, or infrastructure modifications are properly authorized, tested, documented, and monitored.

confidentiality Protection of data from unauthorized disclosure.

COVID-19 The disease caused by a new coronavirus called SARS-CoV-2. It is a potentially severe illness often characterized by fever, coughing, and shortness of breath. The World Health Organization learned of the virus in December 2019.

DTMB Department of Technology, Management, and Budget.

effectiveness Success in achieving mission and goals.

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.*

federal tax information (FTI) Federal tax returns and return information (and information derived from it) in the agency's possession or control which is covered by the confidentiality protections of IRC and subject to the IRC Section 6103(p)(4) safeguarding requirements including IRS oversight. FTI is categorized as sensitive but unclassified information and may contain personally identifiable information.

FTI includes returns or return information received directly from the IRS or obtained through an authorized secondary source, such as the Social Security Administration, the federal Office of Child Support Enforcement, the Bureau of the Fiscal Service, the Centers for Medicare and Medicaid Services, or another entity acting on behalf of the IRS pursuant to an IRC Section 6103(p)(2)(B) Agreement.

FTI includes any information created by the recipient that is derived from federal tax return or return information received from the IRS or obtained through a secondary source.

integrity

Accuracy, completeness, and timeliness of data in an information system.

interface controls

Controls that ensure the accurate, complete, and timely processing of data exchanged between information systems.

internal control

The plan, policies, methods, and procedures adopted by management to meet its mission, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It also includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; violations of laws, regulations, and provisions of contracts and grant agreements; or abuse.

IRC

Internal Revenue Code.

IRS

Internal Revenue Service.

IT

information technology.

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. Our assessment of materiality is in relation to the respective audit objective.

Michigan Integrated Data Automated System (MiDAS)

UIA's computer system used for processing and servicing all unemployment insurance tax and benefit functions.

Michigan Web Account Manager (MiWAM)

UIA's computer system used by unemployment insurance claimants and employers for filing and claim management.

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 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: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud.

rewritten

The recurrence of similar conditions reported in a prior audit in combination with current conditions warrant the prior audit recommendation to be revised for the circumstances.

RSA

A method of multi-factor authentication which utilizes security tokens to generate a single-use log-in personal identification number (PIN).

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.

SOM

State of Michigan.

SQR

Solution Quality Request.

State Unified Information Technology Environment (SUITE)

Statewide guidance to standardize methodologies, procedures, training, and tools for project management and systems development lifecycle management.

System Engineering Methodology (SEM)

A component of SUITE which provides guidance for information systems engineering related project management activities and quality assurance practices and procedures. Use of the methodology will aid in the status tracking, management control, and documentation efforts of a project.

UAT

user acceptance testing.

UIA

Unemployment Insurance Agency.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

OAG

Office of the Auditor General

Independent Objective Transparent

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud
Hotline: (517) 334-8070