Office of the Auditor General
Performance Audit Report

Disaster Recovery of IT Systems

Department of Technology, Management, and Budget

August 2025

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.

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

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit

Disaster Recovery of IT Systems

Department of Technology, Management, and Budget (DTMB)

Report Number:
171-0511-24

Released:
August 2025

A disaster recovery plan (DRP) is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternative site after a disaster. DRPs are created by agency business owners and stored in the Michigan Continuity Management Solution (MiCMS) central repository managed by DTMB. Also, testing scenarios and results are required to be stored in the DRP within MiCMS. In July 2024, there were approximately 370 DRPs and 250 active MiCMS user accounts.

Audit Objective			Conclusion
Objective 1: To assess the sufficiency of DTMB's efforts to monitor the disaster recovery planning process.			Not sufficient
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
DRPs may not be updated or tested annually because the MiCMS Plan Status Dashboard lacks important monitoring information (Finding 1).	X		Agrees
Nearly 70% of IT applications and/or services listed on the State of Michigan Application Prioritization for Recovery (SAPR) did not require a DRP or annual testing. Also, over 300 applications or services did not have an associated DRP on the SAPR (Finding 2).	X		Disagrees
DTMB did not ensure the completeness and accuracy of the SAPR, which could hinder recovery after a large-scale event (Finding 3).		X	Partially agrees

Audit Objective			Conclusion
Objective 2: To assess the sufficiency of DTMB's efforts to evaluate the reasonableness of the elements within the agencies' DRPs.			Not sufficient
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Renewal dates were missing for 92% of DRPs in draft status, indicating the DRPs may need updating and are lacking the necessary information to effectively recover from an event (Finding 4).	X		Partially agrees

Audit Objective	Conclusion
Objective 3: To assess the effectiveness of selected MiCMS access controls.	Effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not have a process to perform annual certifications of MiCMS user accounts (Finding 5).		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

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

August 21, 2025

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

Director Lange and Chief Information Officer Clark:

This is our performance audit report on the Disaster Recovery of IT Systems, 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 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

DISASTER RECOVERY OF IT SYSTEMS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

MONITORING OF THE DISASTER RECOVERY PLANNING PROCESS

BACKGROUND

Sudden, unplanned events can occur which may cause damage or loss to an organization's IT infrastructure. These events can compromise an organization's ability to provide critical functions or services for an extended period of time. Events can be minor, such as a power failure, or they can be major events impacting many applications or services at the same time, such as a fire, natural disaster, or terrorism.

Disaster recovery* planning allows the State to proactively mitigate losses resulting from disaster events and provide for the quick resumption of Mission Essential Functions (MEFs) of an agency. State of Michigan (SOM) agencies are required to create detailed IT disaster recovery plans* (DRPs) and store plans in the Michigan Continuity Management Solution* (MiCMS) centralized repository which is managed by the Department of Technology, Management, and Budget (DTMB).

The SOM has institutionalized the SOM Application Prioritization for Recovery* (SAPR) to identify and prioritize critical applications and services and their recovery in the event of a large-scale outage. Once an application/service goes through the governance, risk, and compliance (GRC) process, which generates a business impact analysis* (BIA) score, and is approved by the Agency Services business relationship manager and agency security officer, the application/service will be listed on the SAPR. SAPR divides applications and services into four tiers based on the following defined support level required for recovery:

- Tier 0 - "Always on" infrastructure required to continue business.
- Tier 1 - Critical agency applications/services requiring recovery as soon as possible.
- Tier 2 - Highly important agency applications/services requiring recovery without long delay.
- Tier 3 - Possibly needed agency applications/services requiring recovery within a specified amount of time.

AUDIT OBJECTIVE

To assess the sufficiency of DTMB's efforts to monitor the disaster recovery planning process.

CONCLUSION

Not sufficient.

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

FACTORS IMPACTING CONCLUSION

- Two material conditions* related to improvements needed in monitoring agency DRPs (Finding 1) and establishing requirements for all tiers of DRPs (Finding 2).
- One reportable condition* related to oversight improvements of the SAPR (Finding 3).
- DTMB established and implemented procedures and workflows within MiCMS for creating and maintaining DRPs.

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

FINDING 1

Improvements needed in DTMB's monitoring of agency DRPs.

DTMB needs to improve its monitoring of agency DRPs to help plan owners ensure SOM information systems are tested annually and up to date. Effective monitoring of DRPs confirms the SOM is prepared and proactive in identifying outdated DRPs and aids in an efficient and effective recovery after a disaster.

The SOM utilizes the MiCMS as a centralized repository for the development and maintenance of all DRPs. SOM Technical Standard 1340.00.070.02 requires agencies to develop and maintain DRPs and the DTMB Director to provide a mechanism for monitoring, reporting, and alerting agency business owners of the plan status for critical IT systems. DTMB created the MiCMS Plan Status Dashboard (Dashboard) to meet both requirements. Currently, MiCMS will notify users before the DRP is set to expire.

Our review noted DTMB did not:

Tiers to identify critical applications and services needing monitoring are not available on the Dashboard.

a. Identify the criticality of the applications and services related to each DRP by indicating the BIA prioritization tier within the Dashboard. The tier for SOM applications and services is critical to monitoring the disaster recovery planning process and is used to determine the requirements for annual testing.

The Dashboard lacks important monitoring information.

b. Provide management and plan owners with the information necessary in the Dashboard to effectively monitor the status of disaster recovery planning and meet the requirements specified by the technical standard. The Dashboard currently lacks important information such as historical evidence of annual DRP updates and dates for the plan owner to perform the next cutover/parallel or walk-through/tabletop test. Without this information on the Dashboard, agencies cannot ensure DRPs meet the testing requirements applicable to their associated tier for the application or service.

   We randomly and judgmentally sampled 22 of 190 DRPs on the Dashboard associated with tier 0 through tier 2 applications or services and noted as of August 22, 2024:

	Total DRPs	DRPs Updated Within the Last 12 Months**	DRPs Tested in the Last 12 Months	Historical Testing Evidence in MiCMS	Cutover or Parallel Testing Performed Timely	Walk-Through or Tabletop Timely Performed
Tier 0	10	2 (20%)	10 (100%)	0 (0%)	10 (100%)	Not applicable
Tier 1	4	0 (0%)	1 (25%)	0 (0%)	1 (25%)	1 (25%)
Tier 2	8	5 (63%)	3 (38%)	1 (13%)	2 (25%)	2 (25%)

** After our review, DTMB and other agencies updated 4 DRPs.

c. Notify MiCMS plan owners when testing requirements are approaching the due date or are overdue. In January 2024, DTMB switched to a new vendor for MiCMS which can capture the data necessary to monitor future due dates and send notifications to DRP owners. At the time of our review, these features had not been fully implemented.

DTMB indicated it is the agencies' responsibility to update and test DRPs annually and meet the requirement for monitoring agency DRPs by creating the Dashboard.

We consider this to be a material condition because of the agencies' exception rate of testing and annual updates and DTMB's critical responsibility to monitor the status of DRPs.

RECOMMENDATION

We recommend DTMB improve its monitoring of agency DRPs.

AGENCY PRELIMINARY RESPONSE

DTMB agrees. Given the length of DTMB's preliminary response, the response and our auditor's comments to Finding 1 are presented on page 24.

FINDING 2

Reevaluation of SOM technical standard for tier 3 applications needed.

DTMB should evaluate SOM Technical Standard 1340.00.070.02 and establish disaster recovery control requirements for all SOM applications and services. DRPs are essential safeguards and they ensure applications can be efficiently restored in the case of a disaster. These safeguards are critical in the case of Statewide outages affecting multiple systems and limited available recovery resources.

SOM has adopted National Institute of Standards and Technology* (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, which allows for the tailoring of security controls.

SOM Technical Standard 1340.00.070.01 states all information systems with a security categorization of "Low," "Moderate," or "High" must have a contingency plan which provides disaster recovery objectives and restoration priorities. The BIA score is used to rank the overall criticality and identifies the level of service criticality. These criticality levels can correlate with the security categorization availability component.

In response to the NIST special publication above, DTMB created SOM Technical Standard 1340.00.070.02 as the tailored security controls. The Standard requires agency directors to ensure all applications supporting MEFs defined in departments' continuity of operations plans (COOPs) have DRPs, in addition to any tier 0, tier 1, and tier 2 applications and services listed on the SAPR. Also, it requires the DTMB Director to develop a strategy ensuring agency DRPs for all applications are tested, reviewed, and revised on an annual basis and to establish plan testing types and minimum time frames.

70% of tier 3 applications on the SAPR did not have a DRP.

As of July 24, 2024, 436 (70%) of the 625 IT applications/services on the SAPR were tier 3 applications. Of the 436 tier 3 applications, 304 (70%) did not have an associated DRP on the SAPR.

SOM Technical Standard 1340.00.070.02 does not establish the minimum contingency planning control requirements which include developing and maintaining contingency plans for systems with tier 3 service availability. As written, the Standard does not address:

a. Tier 3 application requirements to have a current and/or complete DRP; it only recommends a DRP.

b. Annual testing for tier 3 applications. Currently, the Standard does not establish a minimum time frame for parallel or cutover testing; it recommends only the completion of a biennial* tabletop or walk-through test.

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

DTMB believes it has established control requirements and the technical standards to undergo a thorough review process on an annual basis.

In addition, DTMB believes the agencies are responsible for determining if their applications need a DRP. However, this does not address the fact the Standard is deficient as it relates to tier 3 application guidance and does not meet the requirement for the DTMB Director to develop a strategy ensuring agency DRPs for **all** applications are tested, reviewed, and revised on an annual basis consistent with the Standard.

We consider this to be a material condition because of the significant number of tier 3 SOM applications without an associated DRP and the lack of disaster recovery control requirements in the SOM technical standards.

RECOMMENDATION

We recommend DTMB evaluate SOM Technical Standard 1340.00.070.02 and establish disaster recovery control requirements for all SOM applications and services.

AGENCY PRELIMINARY RESPONSE

DTMB disagrees. Given the length of DTMB's preliminary response, the response and our auditor's comments to Finding 2 are presented on page 25.

FINDING 3

Oversight improvements needed for the SAPR.

DTMB should improve its oversight of the SAPR and its related processes to ensure prioritization of applications to be recovered during a large-scale outage.

SOM created the SAPR to identify and prioritize critical applications and their recovery in the event of a large-scale outage. Based on an application's BIA score, the SAPR divides applications and services into four tiers based on the defined support level required for recovery. The higher the BIA score the higher the prioritization ranking. Applications and services with the same BIA scores will have the same prioritization ranking.

Our review of the SAPR noted DTMB did not:

a. Have a process to ensure all critical IT applications and services listed within an agency's COOP are listed in the SAPR. SOM Technical Standard 1340.00.070.01 requires State agencies to identify critical information system assets which support the MEFs. Federal Information System Controls Audit Manual* (FISCAM) recommends periodically reviewing prioritized listings of critical information resources and operations to determine whether current conditions are reflected. Our review of 5 departmental COOPs noted:

   - 1 application listed in the COOP is not listed on the SAPR.

   - 1 COOP had not been updated since 2020.

   - 1 COOP did not identify any critical IT applications.

   Agencies are responsible for completing and maintaining their COOPs and creating DRPs to support MEFs. The implementation of a process would help to ensure the SAPR's completeness and accuracy and could alert agencies when COOPs have not been updated.

b. Have a process to periodically review the application information in the SAPR. After an application is registered in the SOM GRC tool*, the DTMB disaster recovery team (DR team) manually adds the application to the SAPR from the GRC reports. FISCAM recommends the prioritized listing of critical IT resources be periodically reviewed to ensure current conditions are reflected. We reviewed the SAPR as of June 11, 2024 and noted:

   - Three instances of applications possessing the same BIA score with different prioritization rankings on the SAPR.

   - Various clerical errors, such as applications with an incorrect or misspelled agency listed or incorrect plan identification (ID) number.

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

For example:

- 21 applications had different associated MiCMS Plan ID numbers than what was listed in their MiCMS Plan ID number field.
- 4 instances of applications showed related plans that would not be involved in the application's recovery.

These errors could impact disaster recovery efforts to obtain accurate information during a disaster. After we brought this to management's attention, DTMB corrected the clerical errors and updated the SAPR with the correct information.

c. Perform an annual review of the BIA score-to-tier relationship. SOM Technical Standard 1340.00.070.02 requires the DTMB DR team to perform an annual SAPR tier review and evaluate the score-to-tier relationship and properly adjust the scaling to known facts of all production applications. As defined, each review will include an impact assessment of all production applications and services to validate and finalize the score-to-tier relationship. Although the DR team met with stakeholders and DTMB management annually to discuss the tier 0 infrastructure, no discussion of the tier 1 through tier 3 applications or the BIA score-to-tier relationship occurred. Performing the annual review would allow DTMB to:

- Consider relationships between applications and services which could impact the recovery priority.
- Identify mismatches between the application and service tier ranking and its criticality. As of June 11, 2024, the SAPR noted two tier 3 applications in which outage impacts were identified as life-threatening and potentially life-threatening, but the SAPR identified the lowest level of criticality and no risk of personal injury.
- Evaluate the BIA scoring calculation to capture the dynamic nature of the IT environment and ensure all tiers reflect the appropriate service availability for SOM applications and services.

d. Prevent the display of the initial BIA score until the information which determines the score is submitted for review. Displaying the initial BIA score before the review point creates a risk for potential score adjustments to lower the prioritization tier, which dictates disaster recovery planning requirements (see Finding 2). If applications are placed in lower prioritization tiers, SOM may not be adequately prepared in the event of a disaster.

> DTMB states the BIA score calculation is confidential and only a few people know the formula. In addition, the score is finalized after several reviews with final approval from the agency security officer.

For parts a. through c., DTMB maintains it is not the DR team's responsibility to evaluate the SAPR ranking and other information because it is not familiar with the application's business process. However, DTMB needs to improve its oversight of DRPs (see Finding 4). Also, DTMB does not evaluate the prioritization rankings on the SAPR because the prioritization ranking comes from only the BIA score, which is calculated when the application is registered in the GRC tool.

RECOMMENDATION

We recommend DTMB improve its oversight of the SAPR and its related processes.

AGENCY PRELIMINARY RESPONSE

DTMB partially agrees. Given the length of DTMB's preliminary response, the response and our auditor's comments to Finding 3 are presented on page 26.

REASONABLENESS OF ELEMENTS WITHIN THE AGENCIES' DRPs

BACKGROUND

SOM Technical Standard 1340.00.070.02 establishes the SOM strategy for disaster recovery planning by identifying information security advance arrangements and IT structures allowing the SOM to respond to an event so MEFs continue with minimal to no interruption or essential change.

A DRP is a plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. DTMB is required to provide a range of developed disaster mitigation and recovery strategies which allow agencies to confidently restart applications and services. In addition, DTMB is required to provide a mechanism for monitoring, reporting, and alerting agency business owners of the plan status of critical systems to ensure agency DRPs for all applications are tested, reviewed, and revised by the agency on an annual basis and after each major update. The DR team has created the current DRP template within MiCMS for the plan owners. This template includes sections such as assumptions, roles/skills/competencies, plan activation, notification lists, and IT events.

The DR team is tasked with:

- Performing quality checks on DRPs for all tier 0 through tier 2 applications/services within MiCMS to confirm each element within the plan is complete.

- Providing consultation services to agencies to assist in establishing plan strategies and providing guidance in the development of DRPs.

DRPs can be in 1 of 4 different statuses: draft, return, pending approval, and approved. DRPs start in draft status where they can be updated. When completed, they are sent to the DR team for a quality check. After the quality check is performed, if updates are necessary, the DRP is sent back to the plan owner in return status. After the DRP owner makes any updates, the DRP is put in pending approval status for review and approval by the agency plan reviewer. When reviewed and approved, the DRP is in approved status and will have a plan renewal date in one year.

AUDIT OBJECTIVE

To assess the sufficiency of DTMB's efforts to evaluate the reasonableness of the elements within the agencies' DRPs.

CONCLUSION

Not sufficient.

FACTORS IMPACTING CONCLUSION

- One material condition related to improvement needed for DRP oversight (Finding 4).

- DTMB has established and implemented a process to review and provide feedback on agency DRPs.

FINDING 4

Improved oversight of DRPs for SOM IT applications and services needed.

DTMB needs to improve its oversight of DRPs for SOM IT applications and services. Doing so will ensure DRPs are applicable and contain essential information needed for recovery after a disaster.

SOM Technical Standard 1340.00.070.02 requires agencies to develop and maintain DRPs and has established the DR team as a group of subject matter experts tasked with providing consultation services to agencies, assisting them in establishing plan strategies, and providing guidance in the development of DRPs. Also, the DR team monitors agencies' DRPs to track that plans are annually reviewed and revised and to perform quality checks on all tier 0 through tier 2 plans. This is a review to confirm elements within a plan are complete, but it is not an evaluation of the information's appropriateness.

In January 2024, DTMB migrated to a new vendor and all DRPs were placed in draft status unless they were updated in the prior year, with a 2-year window, before automatically archiving the DRP from MiCMS. Placing DRPs into draft status would require agencies to review and confirm their DRPs successfully migrated to MiCMS.

We analyzed data elements displayed on the MiCMS Dashboard for all 370 DRPs, reviewed a sample of 22 DRPs to determine plan completeness, and surveyed MiCMS agency users to gain insight into the DRP process and noted DTMB did not:

a. Monitor agencies' DRPs to ensure:

(1) DRPs are applicable to support current SOM IT applications or services and are not obsolete or duplicative. As of September 16, 2024, 254 (69%) of 370 DRPs in the Dashboard were in draft status and were potentially not needed because of the following indicators:

92% of DRPs in draft status did not have a plan renewal date.

- 234 (92%) did not have plan renewal dates.
- 229 (90%) did not have a test date.
- 42 (17%) had no activity in MiCMS since the DRP migration.

DTMB's process is to review DRPs after the agencies move them within the MiCMS workflow rather than to conduct periodic reviews to identify unneeded DRPs. The term draft status is ambiguous because draft status can also include plans which are being updated. Therefore, it is difficult for DTMB and agencies to truly know which DRPs were previously approved versus currently being updated. DTMB should work with agencies to identify and remove unneeded DRPs.

Important information was missing from DRPs.

(2) Sampled DRPs contain essential plan information. Common missing elements included:

- The primary contacts for declaring an event and activating the DRP. This may include ensuring the primary contacts are on the MiCMS plan notification activation list.

- Restoration procedures and critical roles of staff which include their responsibilities for responding to and resolving a disaster.

- Information to create a self-contained document. Maintaining information in multiple sources is not efficient during a disaster. For example, the recovery time is documented in the system security plan* but is not always included in the DRP.

The DR team stated it does not know the agency business processes or application's architecture because the plan owners are the application's experts. The DR team does not look at the DRP's validity or information appropriateness because team members are experts only in disaster recovery planning strategies. However, as DR subject matter experts, team members are in the best position to review the reasonableness of the DRP elements.

DTMB could utilize its precheck reviews to identify additional areas of recommended training and/or additional workshops to the DRP owners.

DRP template needs updating.

b. Evaluate and update the DRP template to align with NIST and the current SOM IT environment. Our review of DRPs noted:

(1) Template sections might not be applicable and are maintained in other continuity plans. For example, the alternative work site location does not need to be in a DRP because it is the recovery of an application or service. This information is appropriately included in the business continuity plan*.

(2) Tier 0 infrastructure does not have its own template. This type of infrastructure has unique elements which differ from an application or service DRP.

(3) Template sections are outdated and do not reflect the current SOM IT environment. For example,

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

SOM has a virtual environment; however, the backup section of the DRP reflects the traditional server environment.

NIST Special Publication 800-34 Guide recommends DRPs be formatted to provide quick and clear directions if personnel unfamiliar with the plan or the systems are called upon to perform recovery operations. Plans should be clear, concise, and easy to implement in an emergency. A concise and well-formatted template reduces the likelihood of creating overly complex or confusing DRPs.

DTMB asserts the agency can customize the DRP to reflect their business process by removing sections or completing plan parts the agency thinks are necessary. DTMB should work proactively with plan owners on elements, utilizing its experience and knowledge to identify template sections needing updates.

As noted in SOM Technical Standard 1340.00.070.02, the DR team are subject matter experts tasked with providing consultation services to agencies regarding DRPs. Although interpretations vary, a consultant is a person or group who collaborates with teams, typically analyzing a client's current situation and identifying growth opportunities while providing suggestions or improvements. DTMB's interpretation of consultation services is to answer DRP owners' questions about the MiCMS tool, adjusting the template sections, and if requested, have a one-on-one workshop for specific assistance.

Given agencies may not be experts in IT disaster recovery planning, DTMB, as the DRP subject matter experts, should be proactive to ensure DRPs are accurate, complete, and tested and provide additional training, resources, and/or consultation so IT applications/services can be successfully recovered in the event of a disaster.

We consider this to be a material condition because a significant number of plans were in draft status and agency reliance on the DRP template as the primary guidance for creating DRPs.

RECOMMENDATION

We recommend DTMB improve its oversight of DRPs.

AGENCY PRELIMINARY RESPONSE

DTMB partially agrees. Given the length of DTMB's preliminary response, the response and our auditor's comments to Finding 4 are presented on page 28.

SELECTED ACCESS CONTROLS

BACKGROUND

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

The primary users of MiCMS consist of agency plan owners, agency plan reviewers, and the DTMB DR team.

AUDIT OBJECTIVE

To assess the effectiveness* of selected MiCMS access controls.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- DTMB has established and implemented some user access controls within MiCMS in accordance with State policy, such as defining the process for requesting and approving user access.
- One reportable condition related to establishing a process to perform annual certifications (Finding 5).

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

FINDING 5

Improvements needed for MiCMS annual user access certification.

DTMB should establish a process to perform annual certifications of MiCMS user accounts to ensure user accounts are appropriate and have the correct level of access.

SOM Technical Standard 1340.00.020.01 requires account managers to implement an annual review of accounts to verify they are still required and compliant with the account settings and access permissions.

In January 2024, DTMB switched vendors for MiCMS and migrated all DRPs and associated users. During our review, we noted DTMB did not conduct or document it conducted an annual certification for MiCMS users who had access for more than one year.

DTMB provided us with the DR team quarterly newsletter which included a reminder to perform an annual review of users. Users were required to complete the new MiCMS training before their account was migrated to assign a license and access their account. However, no requirement exists for authorizing agents to acknowledge and document all users were still appropriate and had the correct level of access.

RECOMMENDATION

We recommend DTMB establish a process to perform annual certifications of MiCMS user accounts.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees it should establish a formal process to require the recertification of user's access to MiCMS accounts.

DTMB will develop a written procedure no later than September 30, 2025, and will implement the recertification procedure by December 2025.

AGENCY PRELIMINARY RESPONSES

DISASTER RECOVERY OF IT SYSTEMS
Department of Technology, Management, and Budget

Finding 1 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DTMB's preliminary response to Finding 1 and our auditor's comments providing further clarification and context where necessary.

Overall Auditor's Comment

As the technology expert for the State of Michigan, DTMB is responsible for ensuring applications and services are available after a disaster. In the agency preliminary response below, DTMB deflects its responsibility to the agencies for the monitoring and oversight of the DRPs to confuse the reader on its responsibilities regarding disaster recovery. We acknowledge the agencies' role in the disaster recovery process; however, this finding reflects DTMB's insufficient effort in monitoring the DRP process.

Finding 1: Improvements needed in DTMB's monitoring of agency DRPs.

DTMB provided us with the following response:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
DTMB agrees the DR plan status dashboard reporting can be enhanced to help plan owners ensure their DR plans are up-to-date and tested annually. The DR plan status dashboard reports the plan status, based on data that is required by standard to be contained within DRs in the Michigan Continuity Management Solution (MiCMS).	
DTMB developed the existing dashboard to help plan owners monitor the status of their DR plans. In 2023, DTMB identified the need to update the existing SOM DR plan status dashboard. DTMB deferred the development of an updated dashboard while DTMB procured and implemented a new tool for DR plans to ensure the new tool was implemented on schedule. This allowed for efficient use of SOM state resources to evaluate the tool's enhanced reporting capabilities prior to developing a new dashboard.	Although the dashboard assists agencies in determining the status of their DRPs, it was primarily developed because the Standard requires DTMB to monitor agencies' DRPs. DTMB's response only addresses its responsibility to provide agencies with information, it is silent as to DTMB's plan to meet its required monitoring and report responsibilities which is critical to addressing the high exception rates we noted for testing and the annual updates to DRPs.
To assist agency DR Plan owners to ensure their DR plans are up-to-date and tested annually, DTMB began updating the existing plan status dashboard in the fall of 2024. DTMB anticipates the updated dashboard, as deemed appropriate by DTMB, will be completed by October 31, 2025.	We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 1

Go to Finding 2

Finding 2 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DTMB's preliminary response to Finding 2 and our auditor's comments providing further clarification and context where necessary.

Overall Auditor's Comment

See Overall Auditor's Comment for Finding 1.

Finding 2: Reevaluation of SOM technical standard for tier 3 applications needed.

DTMB provided us with the following response:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
DTMB disagrees. DTMB established disaster recovery minimum contingency planning control requirements for all applications in the State of Michigan's 1340.00.070.02 Information Technology Disaster Recovery Planning Standard. Tier 1 and Tier 2 applications are deemed "most critical" and "highly important" to the State of Michigan, respectively. Tier 3 applications are only deemed "possibly needed" and as such do not have the same DRP or testing requirements. SOM Standard 1340.00.070.02 recommends Tier 3 applications have a DRP but does not require one.	DTMB is minimizing the importance of tier 3 applications which account for approximately 70% of the State's applications. Some of the tier 3 applications have an impact on the State's citizens and include payment systems for Treasury, Michigan Department of Education, and Michigan Department of Health and Human Services which seem important to the department's business operations.
Additionally, the DTMB director has met the requirement in the standard to "develop a strategy ensuring agency DRPs for all applications are tested, reviewed, and revised on an annual basis consistent with the Standard" by establishing the SOMs 1340.00.070.01 and 1340.00.070.02 standards which includes the accountable and responsible parties and the requirements for the applications. *SOM Standard 1340.00.070.02 requires "each agency to define those components that are essential to continuing their critical business operations for the SOM and document them accordingly". Based on this language in the SOM 1340.00.070.02 Standard, DTMB accepts the risk state agencies may elect to not develop a disaster recovery plan for Tier 3 applications because each agency has the authority.*	DTMB states it met the requirement to develop a strategy for **all** applications**;** however, DTMB did not meet the Standard because it currently does not require tier 3 applications to have a DRP. Therefore, DTMB could not have developed a strategy for all. DTMB's response to Finding 3, subpart d., acknowledges it is part of the final approval process for the BIA score. As such, the agencies are not independent in determining the BIA score. Therefore, DTMB's role affects the application tier and, consequently, if a DRP is required. Because DTMB established a Standard that does not require a DRP for tier 3 applications, it incentivizes the agencies to answer the questions in such a way which would result in a tier 3 classification and, therefore, not requiring a DRP even if the application is important to their business operations.

We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 2

Go to Finding 3

Finding 3 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DTMB's preliminary response to Finding 3 and our auditor's comments providing further clarification and context where necessary.

Overall Auditor's Comment

See Overall Auditor's Comment for Finding 1.

Finding 3: Oversight improvements needed for the SAPR.

DTMB provided us with the following response:

AGENCY PRELIMINARY RESPONSE

DTMB partially agrees.

For subpart a., DTMB disagrees. DTMB disagrees creating a new process is necessary given the existing responsibilities outlined in current state standards and policies.

Per the Administrative Guide to State Government, 0240.08 Continuity of Operations (COOP) Plan, and SOM Standard 1340.00.070.02, each agency is accountable and responsible for identifying the information systems which support their mission essential functions. Additionally, SOM Standard 1340.00.070.02 requires each agency to create IT DR Plans for all applications supporting Mission Essential Functions (MEF) defined in the department's Continuity of Operations (COOP) plan.

In accordance with SOM Standard 1340.00.070.02, each agency director is responsible for ensuring the BIA is completed and approved for their applications. If an agency completes the BIA process as required, the application will be included on the SAPR.

DTMB is not responsible for the oversight of state agencies; rather DTMB is responsible for consulting with state agencies as needed. As part of DTMB's existing COOP precheck review process, DTMB reviews agency COOPs to determine if the MEFs contained in the plan identify the applications that support their MEF(s). DTMB utilizes functionality within MiCMS' BCM Admin Quality PreCheck to notify plan preparers when there are gaps in a COOP, including identification of the applications supporting the MEFS, before the COOP is approved by the plan owner.

For subpart b., DTMB agrees it did not have a formal process to periodically review the application information in the SAPR listing. As noted in the finding, DTMB corrected the clerical errors.

DTMB is replacing the manual process with an automated process which will import the needed data from the data source into the SAPR, reducing the risk of clerical errors. DTMB anticipates the automated process will be completed by October 31, 2025.

AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE

The current process does not ensure all critical applications are on the SAPR. One agency's COOP had not been updated since 2020. As the owner of the SAPR, DTMB should ensure the completeness of the list.

DTMB appears to cite the Standards to bolster its argument that State agencies are solely responsible for monitoring and oversight of the SAPR and related processes. This does not change our conclusion or interpretation of the Standard cited in the Finding requiring DTMB to improve its oversight of the SAPR and related processes.

DTMB states it is completing precheck reviews but based on the exceptions noted in subpart a., the precheck process does not appear to be working sufficiently; therefore, DTMB needs to implement a process to ensure the accuracy and completeness of the SAPR.

For subpart c., DTMB agrees it did not formally document results of the annual review of the BIA score to tier relationship for Tiers 1 - 3. DTMB will document the review in the future following the State standard. DTMB expects the next annual review will occur in December 2025.

For subpart d., DTMB disagrees. DTMB disagrees displaying the BIA score before the SSP approval point creates an undue risk for potential score adjustments to lower an application's prioritization tier. The inputs for the BIA score and the resultant BIA score are reviewed and approved by personnel different than the individuals who input the information, maintaining separation of duties. The MCS Liaisons review all of the application specific information, including data classification and impact, for reasonableness. Then the Agency Security Officer and the appropriate DTMB leadership review and approve the inputted information and the resultant BIA score. The separation of duties significantly reduces the risk that an individual would answer the BIA questions in such a manner as to inappropriately manipulate the outcome of the BIA calculation so a DRP would not be required.

DTMB has implemented sufficient compensating controls to reduce the risk via the separation of duties. DTMB accepts the residual risk.

This issue exists due to the lack of requirements for tier 3 applications (see Finding 2). Also, although more than one individual is involved in determining the BIA score, seeing the BIA score provides the opportunity for inadvertent or intentional adjustments to the scoring questions which can lower the BIA score and impact the tiering level. For instance, we identified 80 tier 3 applications with BIA scores within .25 points from being classified as tier 2 and required to have a DRP. Changing the BIA score to populate after the questions are submitted for review reduces the risk of scoring manipulation.

We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 3

Go to Finding 4

Finding 4 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DTMB's preliminary response to Finding 4 and our auditor's comments providing further clarification and context where necessary.

Overall Auditor's Comment

See Overall Auditor's Comment for Finding 1.

Finding 4: Improved oversight of DRPs for SOM IT applications and services needed.

DTMB provided us with the following response:

AGENCY PRELIMINARY RESPONSE

DTMB partially agrees.

For subpart a1., DTMB partially agrees. DTMB agrees the State did not formally assign accountability within the SOM Standards for state agencies to validate if their DR plans are obsolete, duplicative, or not needed. Although accountability was not formally assigned, it was implied.

Per SOM standards, state agencies are accountable for ensuring agency DRPs are developed, updated, and approved. Since state agencies are accountable for developing, updating, and approving their DR plans, state agencies (including DTMB) are accountable to monitor that their DR plans are applicable; therefore, DTMB does not agree it is solely accountable for monitoring/oversight of agency DR plans.

DTMB will update the SOM standard to formally assign accountability to archive DRPs that are obsolete (October 31, 2025). State agencies may archive DRPs that are obsolete, duplicative or not needed using the existing process.

To assist in identifying and archiving obsolete DR plans, the new MiCMS tool implemented in January of 2024, automatically archives DR plans that remain in draft status without being updated and approved for 2 years.

The numbers contained in the finding include Tier 3 applications which do not require a DRP. See DTMB's response to finding 2.

For subpart a2., DTMB disagrees all elements within the SOM DRP template are required to be contained within a completed application layer DRP.

The contents of a DRP are modifiable for the specific information system and its architecture to align with the IT support environment and agency business needs. As such, DTMB does not require each element in the DRP template be used or contained within the completed DRP.

AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE

The Standard clearly assigns DTMB the monitoring responsibility of the DRP process. To meet the requirement, DTMB created the MiCMS dashboard as the mechanism to monitor, at a minimum, tier 0 through tier 2 DRPs. However, the dashboard also contains tier 3 DRPs which are not "required" and account for a considerable number of the DRPs in "draft status." "Implied" accountability does not represent a sound internal control process; it must be clearly articulated so all parties understand their roles and responsibilities. As the owner of the dashboard, DTMB is responsible for monitoring all of the contents of the dashboard; if it had done so, duplicative or obsolete DRPs would have been identified and communicated to the agencies (see Finding 2).

The audit finding did not state DTMB is solely accountable for monitoring/oversight of agency DRPs. See overall auditor's comment for Finding 1.

There is no opportunity for the agencies to remove a section which is not applicable. Instead, the option is to leave it blank. The DRP template should contain baseline information beyond the generic wording to support how the application will be recovered. Primary contacts, restoration procedures, and critical roles are all critical elements which should not be blank in a DRP.

The DTMB DR team, who manages the DRP tool, is responsible for performing a "quality check" to "confirm each element within the plan is complete" per SOM Standard 1340.00.070.02. The DR Team uses practical professional experience in their quality check and conducts a gap analysis reviewing the DRPs for common elements needed within a DRP. The DTMB DR team utilizes functionality within MiCMS' BCM Admin Quality PreCheck to notify plan preparers when there are gaps in an application layer DRP before the DR plan is approved by the plan owner. Per the SOM Standard 1340.00.070.02, the DR Team's "quality check does not substitute the review of each plan. Each agency is still responsible to complete in-depth review and approve plan updates."

DTMB states it uses practical, professional experience in performing quality prechecks and gap analysis; however, these tasks only identify incomplete sections in a DRP and are not an evaluation or reasonableness check of the plan information. While we agree DTMB would not know the specifics of each agency's business process, its professional experience in disaster recovery should be able to identify when information contained in a DRP is not adequate or reasonable for application recovery after a disaster.

To assist state agencies in preparing DRPs, the DTMB DR team regularly provides consultative services to state agencies upon their request, including both scheduled workshops and unscheduled calls. The consultative services are to assist agencies in the development of their plans; however, the DR team are not experts in each information system and its architecture or the agency business processes. The experts in an information system and business process and its architecture are the plan owners and the system's support team. Therefore, the review and approval of a DRP has been assigned to the respective agency management or their delegee per the SOM Standard.

DTMB still has a role in the approval process of the DRPs. As such, the DR team should exercise its professional experience and judgment when DRP information seems inadequate or incomplete.

As the experts in an information system and its business process and architecture, SOM standards 1340.00.070.01 and 1340.00.070.02 require the agency information system owner or their designee to review and approve their DR plans. The approval indicates the contents of the DRP is appropriate for the application.

Agencies are the experts on their business processes; however, their applications are supported by DTMB's Agency Services, who provides expertise in the information system architecture. The DR team will not evaluate the agencies' content even though it may lack appropriateness in comparison to similar applications. See overall auditor's comment for Finding 1.

DTMB agrees with the need to update the DRP template to align with the current SOM IT environment and the state's business needs. DTMB is updating the DRP template (see DTMB's response to subpart b). DTMB does not agree that all the elements identified by the OAG as missing from a DRP are always required or required to be within the DRP. A DRP is situational and needs to be tailored to the specific application's environment and agency needs.

For subpart b., DTMB agrees with the need to update the DRP template to align with the current SOM IT environment and the state's business needs. DTMB is updating the current DRP template as DTMB deems it necessary to align with the current SOM IT environment and the state's business needs. NIST 800-34, is guidance established for federal agencies to consider and is not required for use by non-federal entities; however, DTMB will review and consider this guidance. DTMB expects the updated template will be available for use for new DRPs beginning January 31, 2026.

Although NIST was developed for federal agencies and they are required to use it, many other governmental and private entities, like the State of Michigan, have chosen to adopt NIST. Because DTMB has already aligned its standards with NIST 800-53, it makes sense to utilize the additional guidance NIST 800-34 provides related to various IT-related topics as outlined in the Finding.

We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 4

Go to Finding 5

PROGRAM DESCRIPTION

A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternative site after a disaster. DRPs are created by business owners and stored in the MiCMS central repository managed by DTMB. Also, testing scenarios and testing results are required to be stored in the DRP within MiCMS. In July 2024, there were approximately 250 active MiCMS user accounts and 370 DRPs. As of July 29, 2024, the DR team had 6 employees.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine DTMB's processes for monitoring and evaluating DRPs. 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.

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, 2022 through October 31, 2024.

METHODOLOGY

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

- Reviewed SOM policies, standards, procedures, and best practices related to DRPs and access controls.

- Interviewed DTMB management and staff to gain an understanding of the disaster recovery process.

- Reviewed system documentation related to DRPs and quality checks.

- Performed a preliminary data analysis of DRPs and fiscal year 2023 Statewide Integrated Governmental Management Applications* (SIGMA) expenditures related to disaster recovery.

OBJECTIVE 1

To assess the sufficiency of DTMB's efforts to monitor the disaster recovery planning process.

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

To accomplish this objective, we:

- Randomly and judgmentally sampled 22 of the 190 DRPs as of June 11, 2024 with a tier of 0 through 2 from the Dashboard to determine whether:
    - SOM DRPs were being updated and tested annually within MiCMS.
    - DTMB was monitoring tier 1 and tier 2 DRPs for their annual update, review, and appropriate testing type.
- Judgmentally sampled 5 of the 27 COOP 's from the Dashboard as of July 24, 2024 to determine if all critical IT systems identified on each COOP were reflected on the SAPR.
- Reviewed the completeness and accuracy of the Dashboard and SAPR.
- Reviewed the BIA scoring process.
- Evaluated the prioritization of applications and services on the SAPR.
- Surveyed 335 MiCMS users as of August 21, 2024 and reviewed the 133 responses received.
- Reviewed the MiCMS newsletters, communications, and FAQ library.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. Our judgmental samples were selected based on risk and to ensure significant State government operations within the population were sufficiently reviewed. For our judgmental samples, we could not project the results to the respective populations.

OBJECTIVE 2

To assess the sufficiency of DTMB's efforts to evaluate the reasonableness of the elements within the agencies' DRPs.

To accomplish this objective, we:

- Randomly and judgmentally sampled 22 of the 190 DRPs with a tier of 0 through 2 as of June 11, 2024 to determine if the necessary disaster recovery information was documented within each plan, including applicable loss scenarios and disaster recovery servers as of September 26, 2024.
- Judgmentally sampled 6 of 10 tier 0 DRPs to validate the existence of a back-up DRP as of June 11, 2024.

- Analyzed data elements displayed on the Dashboard for all 370 DRPs as of September 16, 2024.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. Our judgmental samples were selected based on risk and to ensure significant State government operations within the population were sufficiently reviewed. For our judgmental samples, we could not project the results to the respective populations.

OBJECTIVE 3

To assess the effectiveness of selected MiCMS access controls.

To accomplish this objective, we:

- Reviewed all 259 MiCMS users as of July 16, 2024 to determine and verify:
  - Access was granted prior to receiving appropriate training.
  - Users were active State employees or contractors.
- Randomly and judgmentally sampled 26 of the 253 non-administrator users with an active MiCMS license, as of July 16, 2024, to determine whether DTMB:
  - Maintained and properly approved access request forms.
  - Granted access to MiCMS users based on the roles requested on the access request forms.
  - Recertified user roles and access.
- Randomly and judgmentally sampled 22 of the 190 DRPs as of June 11, 2024 with a tier of 0 through 2 from the Dashboard to:
  - Compare all 26 users named as authorized activators* listed in the MiCMS plan activation notification list to determine if the authorized activators were the same.
  - Review all 88 users named as of July 16, 2024 to determine if the users had access to MiCMS.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. Our judgmental samples were selected based on risk and to ensure significant State government operations within the population were sufficiently reviewed. For our judgmental samples, we could not project the results to the respective populations.

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

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 it agrees with 2 of the recommendations, partially agrees with 2 of the recommendations, and disagrees with 1 recommendation.

The agency preliminary response following each recommendation in our report was taken from the agency's 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 3, 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 December 2016 performance audit of Disaster Recovery and Business Continuity* of IT Systems, Department of Technology, Management, and Budget (071-0511-15):

Prior Audit Finding Number	Topic Area	Current Status	Current Finding Number
1a	Infrastructure DRP development.	Rewritten*	4
1b	Applications and services prioritization.	Complied	Not applicable
1c	Recovery time objectives and recovery point objectives testing.	Not in scope of this audit.	
2a	Red Card included all critical systems.	Rewritten	3
2b	Addition, removal, and reclassification of systems on the Red Card.	Complied	Not applicable
3	DTMB and agency coordination of DRP preparation.	Not in scope of this audit.	
4a	DRP necessary documentation.	Rewritten	4
4b	Business continuity plan critical elements for State's 3 hosting centers.	Not in scope of this audit.	
5	Disaster recovery servers on Red Card.	Complied	Not applicable
6	Maintaining Living Disaster Recovery Planning System* access.	Rewritten	5
7a	DRPs stored in Living Disaster Recovery Planning System.	Complied	Not applicable
7b	DRP backup locations.	Complied	Not applicable
8	Effective DRP version control.	Complied	Not applicable

* Business continuity plans were not included in the audit scope.

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

GLOSSARY OF ABBREVIATIONS AND TERMS

access controls

Controls protecting data from unauthorized modification, loss, or disclosure by restricted access and detecting inappropriate access attempts.

auditor's comments to agency preliminary response

Comments the OAG includes in an audit report to comply with *Government Auditing Standards*. Auditors are required to evaluate the validity of the audited entity's response when it is inconsistent or in conflict with the findings, conclusions, or recommendations. If the auditors disagree with the response, they should explain in the report their reasons for disagreement.

authorized activator

Any person listed as someone eligible to activate a DRP.

biennial

every two years.

business continuity plan

Documentation of a predetermined set of instructions or procedures describing how an organization's mission/business process will be sustained during and after a significant disruption.

business impact analysis (BIA)

A scoring and tier scheme outlining a quantitative approach to application scoring for the enterprise. Scores establish recovery priorities in the event of a disaster and define minimum support requirements for tier 0, tier 1, and tier 2 SAPR applications and services. The collective evaluation produces an overall score of 1 through 10 and is used to run the application's recovery sequence.

continuity of operations plan (COOP)

An effort within the Executive Office to ensure that mission essential functions (MEF) continue to perform during disruption of normal operations. This is a department-level, pro-active plan that facilitates the rapid recovery of business operations to reduce the overall impact of the disaster, while ensuring the continuity of the critical business functions during and after a disaster, assuming IT is up and available.

Dashboard

MiCMS Plan Status Dashboard.

disaster recovery

The technical aspect of business continuity which includes the use of resources and activities to reestablish IT services (including components such as infrastructure, telecommunications, systems, applications, and data) at an alternate site following a disruption of IT services. Disaster recovery includes subsequent resumption and restoration of operations at a more permanent site.

disaster recovery plan (DRP)

A plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

DR team

disaster recovery team.

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*.

GRC

governance, risk, and compliance.

GRC tool

The tool used by the agency information system owner to document their risk assessment.

ID

identification.

internal control

The plan, policies, methods, and procedures adopted by management to meet its mission, strategic plan, 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.

IT

information technology.

Living Disaster Recovery Planning System

An IT system used by DTMB to create, store, and maintain the States's DRPs and business continuity plans. DTMB migrated away from this system in May 2018.

material condition

A matter, in the auditor's judgment, which 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.

MEF

Mission Essential Function.

Michigan Continuity Management Solution (MiCMS)

A secure, centralized repository for development and maintenance of all DRPs.

National Institute of Standards and Technology (NIST)

An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.

performance audit

An audit which 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.

reportable condition

A matter, in the auditor's judgment, 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 warranting the prior audit recommendation to be revised for the circumstances.

SOM

State of Michigan.

State of Michigan Application Prioritization for Recovery (SAPR)

A list identifying critical systems and recovery prioritization in the event of a large-scale disruption. All applications having a completed System Registration and Profile (SRP) in the State's GRC tool will be listed on the SAPR.

Statewide Integrated Governmental Management Applications (SIGMA)

The State's enterprise resource planning business process and software implementation suite supporting budgeting, accounting, purchasing, human resource management, and other financial management activities.

system security plan	An overview of the information system and security requirements and description of the controls in place to provide the appropriate level of security.

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