Office of the Auditor General
Performance Audit Report

Disaster Recovery and Business Continuity of IT Systems

Department of Technology, Management, and Budget

December 2016

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

071-0511-15

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit
Disaster Recovery and Business Continuity of IT Systems
Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0511-15

Released:
December 2016

A business continuity plan (BCP) documents the procedures for sustaining an organization's business processes during and after a disruption to IT services. An entity should identify its critical business processes and complete a BCP for each process as well as a disaster recovery plan (DRP) to define the resources, actions, tasks, and data required to recover the technology. DTMB works with State agencies to complete the DRPs and BCPs to help ensure that the State's critical systems can be timely recovered in the event of a disaster.

Audit Objective	Conclusion
Objective: To assess the effectiveness of the State's efforts to develop and maintain DRPs and BCPs for State of Michigan business functions supported by IT systems.	Not effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not fully plan to restore all Red Card systems (those considered critical infrastructure services and enterprise systems) in the event of a Statewide IT disaster. Unless restored, many of these systems will be unavailable within the 24-hour maximum recovery time needed for Red Card systems (Finding #1).	X		Agrees
DTMB did not ensure the completeness and accuracy of the Red Card, which could lead to recovery resources not being directed to the most critical systems and services first (Finding #2).	X		Agrees
DTMB and State agencies did not always coordinate the preparation of DRPs and BCPs. Plans were not always created and did not adequately address recovery of both the business process and the information system (Finding #3).	X		Agrees

Findings Related to This Audit Objective (*Continued*)	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not implement a review process to ensure that DRPs and BCPs contained the necessary elements for effective disaster recovery (DR). Relying on plans that are missing critical information can delay recovery of critical systems and business processes (Finding #4).	X		Agrees
DTMB did not ensure that DR servers were in place for all Red Card systems. An incident at a hosting center could significantly delay recovery time for these critical systems if DR servers are not in place (Finding #5).		X	Agrees
DTMB, in conjunction with State agencies, did not grant and maintain appropriate access to the DRPs stored in the Living Disaster Recovery Planning System. DTMB and agency staff need access to ensure that plans can be updated and retrieved in a timely manner to expedite restoring the systems (Finding #6).		X	Agrees
DTMB and State agencies did not fully utilize a central repository and backup storage location for DRPs and BCPs to ensure that plans are readily available in the event of a disaster (Finding #7).		X	Agrees
DTMB and State agencies did not implement effective version control for DRPs and BCPs to ensure use of the correct version for updating or execution in a disaster (Finding #8).		X	Agrees

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

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

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

OAG
Office of the Auditor General

Doug A. Ringler, CPA, CIA
Auditor General

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

December 15, 2016

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

Dear Mr. Behen:

I am pleased to provide this performance audit report on Disaster Recovery and Business Continuity of IT Systems, Department of Technology, Management, and Budget.

Your agency provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and submit it within 60 days of the date above to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

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

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

TABLE OF CONTENTS

DISASTER RECOVERY AND BUSINESS CONTINUITY OF IT SYSTEMS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

DEVELOPING AND MAINTAINING DISASTER RECOVERY PLANS* (DRPs) AND BUSINESS CONTINUITY PLANS* (BCPs)

BACKGROUND

Sudden, unplanned events can occur that cause damage or loss to an organization. These events can compromise an organization's ability to provide critical functions or services for an extended period of time, causing management to invoke its DRPs and BCPs. Incidents can be minor, such as a power failure, or major events, such as a fire, natural disaster, and terrorism.

A DRP is a written plan for recovering information systems at an alternate facility in response to a major hardware or software failure or facility destruction.

A BCP documents the procedures for sustaining an organization's business processes during and after a significant disruption to business operations, including disruptions to an IT system. State agencies are responsible for preparing BCPs for their critical business functions.

The Department of Technology, Management, and Budget (DTMB), in conjunction with State agencies, established a list of the State's most critical systems and infrastructure services known as the Red Card*. Red Card systems are classified into three categories that determine the order in which the systems would be restored. Changes to the Red Card are made by the disaster recovery* (DR) team when a DTMB Agency Services manager submits a DTMB-208 form. As of December 2015, the Red Card contained 84 critical systems and infrastructure services from the State's more than 1,700 systems and services.

DTMB Administrative Guide policy 1390 requires that agencies develop BCPs for continuing the operation of essential business processes and ensure that critical systems have a DRP and are included on the Red Card. The loss of essential business processes could affect the safety, health, subsistence, and welfare of the public and impact State government operations.

The Federal Information System Controls Audit Manual* (FISCAM) is a methodology for performing information system control audits published by the U.S. Government Accountability Office (GAO).

The National Institute of Standards and Technology* (NIST) standards are recommended guidelines for implementing information system security controls.

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

AUDIT OBJECTIVE	To assess the effectiveness* of the State's efforts to develop and maintain DRPs and BCPs for State of Michigan business functions supported by IT systems.
CONCLUSION	Not effective.
FACTORS IMPACTING CONCLUSION	• Four material conditions* related to incomplete IT disaster planning; improved completeness and accuracy of the Red Card; lack of coordination of DRP and BCP preparation; and lack of a review process for DRPs and BCPs (Findings #1 through #4). • Four reportable conditions* related to lack of DR servers, limited accessibility of DRPs in DTMB's repository, improved storage of DRPs and BCPs, and ineffective version control (Findings #5 through #8). • DTMB established redundant, physically separate hosting center facilities to reduce the amount of time needed to restore critical systems and infrastructure services after a disaster.

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

FINDING #1

More complete IT disaster planning needed.

DTMB did not fully plan to restore all critical infrastructure services and enterprise systems necessary to restore the other Red Card systems in the event of a Statewide IT disaster. As a result, the State may not be able to restore all critical infrastructure services and systems within the maximum recovery time of 24 hours for Red Card systems.

FISCAM states that an entitywide plan should identify all critical systems and resources needed to recover and support those systems. In addition, NIST states that critical infrastructure components, such as the telecommunications network, should be addressed by the plan.

DTMB developed plans for recovering from significant events that would impact the mainframe systems and minor incidents that would impact a single system; however, it had not developed a plan to recover from a serious disaster that would impact many or all of the State's IT resources.

Planning for restoration of critical IT infrastructure not complete.

DTMB did not:

a. Sufficiently develop recovery plans for infrastructure services needed to restore the State's IT environment. Specifically:

   (1) DTMB did not fully plan for the restoration of the network. The network is the underlying infrastructure for the State's IT environment, consisting of multiple computer systems and hardware that allow the sharing of information. The network is redundant, which reduces the likelihood of it becoming completely inaccessible; however, if the network is unavailable, users will be unable to access the majority of the State's IT systems.

   DTMB had a partial plan for recovering the network; however, the plan was stored on the network, making it inaccessible if the network is down.

   (2) DTMB did not identify the State's Intranet as a critical infrastructure service and fully plan for its restoration. Many of the State's critical systems and services, including the Living Disaster Recovery Planning System (LDRPS), are accessed through the Intranet. If unavailable, DTMB and State agencies will not be able to access LDRPS, which contains the DRPs and BCPs for some of the State's critical information systems. DTMB developed a DRP for the Intranet; however, it had not been updated or tested since 2011.

Enterprise systems not properly prioritized for restoration.

b. Properly prioritize enterprise systems, such as Active Directory* and LDRPS, in its recovery priorities. For example:

   (1) DTMB's DRPs give priority to the recovery of 27 systems prior to its recovery of Active Directory. Active Directory is a system that manages usernames and passwords necessary to log in to many of the State's critical systems and services, including the State's network and Intranet. Without first recovering Active Directory, users will be unable to access many of those 27 systems.

   (2) DTMB's plans specify the recovery of 21 systems prior to the recovery of LDRPS. LDRPS is the State's central repository for creating, updating, and storing DRPs and BCPs needed to restore systems and services. Recovery of those 21 systems whose DRPs and BCPs are stored in LDRPS may be delayed because the plans will be inaccessible until it is restored.

   (3) Eighteen systems shared the highest restoration priority. Without further ranking these 18 systems, DTMB may not accurately and timely determine which systems to recover first.

c. Perform testing or other analyses to ensure that recovery time objectives* and recovery point objectives* could be met for infrastructure services and systems in the event of a disaster impacting multiple systems.

   According to DTMB, recovery time objectives and recovery point objectives were established assuming that only one system would need to be restored. DTMB did not plan for multiple system failures, such as a disaster impacting an entire hosting center.

DTMB Data Center Operations relies on DTMB teams to request that the systems and services be added to the Red Card and to properly classify them for recovery. DTMB informed us that it was not aware that critical systems and services relied on the Intranet.

RECOMMENDATION

We recommend that DTMB fully plan to restore critical infrastructure services and enterprise systems necessary to restore the other Red Card systems in the event of a Statewide IT disaster.

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

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and plans to restore all critical infrastructure services and enterprise systems necessary to restore the other Red Card systems in the event of a Statewide IT disaster. BCPs and DRPs for all critical infrastructure systems and enterprise systems will be completed and maintained. In addition, more comprehensive test plans from an enterprise view will be developed and tests will be scheduled on a regular basis.

FINDING #2

Completeness and accuracy of the Red Card should be improved.

DTMB did not ensure the completeness and accuracy of the Red Card, which could lead to recovery resources not being directed to the most critical systems and services first.

FISCAM recommends that DRPs specify recovery priorities, including the order for restoring the systems. The prioritized listing of critical IT systems and services should be periodically reviewed and approved by management to ensure that it reflects current conditions.

DTMB created the Red Card to identify critical IT systems and services to help direct disaster recovery efforts on the most critical systems first. As of December 2015, the Red Card included 72 systems and 12 IT infrastructure services.

DTMB did not:

a. Evaluate, in conjunction with State agencies, whether all agency-identified critical systems, including vendor-managed and vendor-hosted systems, were appropriately on the Red Card.

Critical systems not on the Red Card.

We compared the Red Card systems with partnership agreements between DTMB and 8 agencies and noted that only 17 of the 44 critical systems identified in the partnership agreements were on the Red Card. We also identified 2 Red Card systems that were not listed in the partnership agreements. DTMB and the agencies gave the following reasons why some critical systems were not on the Red Card:

(1) Some agency staff and DTMB Agency Services staff believe that the Red Card should contain only those systems that are critical to the State as a whole, whereas other agency staff believe that the Red Card should contain all critical systems, including those that impact only one agency.

According to Red Card criteria, systems that directly impact critical business functions for one agency or a small number of users should be included on the Red Card.

(2) Critical vendor-managed and vendor-hosted systems are inconsistently included on the Red Card by State agencies. As of December 2015, the Red Card contained 9 vendor-managed and vendor-hosted systems; however, some vendor systems were not included on the Red Card because the vendor is responsible for restoring them in the event of a disaster.

DTMB informed us that vendor-managed and vendor-hosted systems should be on the Red Card

because DTMB would need to reestablish access to the systems.

b. Require agency management approval when systems were added to, removed from, or reclassified on the Red Card.

In addition, DTMB did not periodically review the Red Card for accuracy. For example, one system was misclassified because agency management was not sufficiently involved in the process of adding and classifying the system on the Red Card and there was no periodic review to ensure that the classification remained accurate.

DTMB should work with each agency to ensure that the Red Card contains all critical systems. DTMB informed us that hardware, backup, and support costs incurred for Red Card systems may deter agencies from adding their systems to the Red Card.

RECOMMENDATION

We recommend that DTMB ensure the completeness and accuracy of the Red Card to help ensure that recovery efforts are devoted to the most critical systems and services first.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will work with State agencies to ensure the completeness and accuracy of the Red Card by determining the most critical systems and services for their inclusion on the Red Card. DTMB will assist State agencies in completing a business impact analysis to identify critical applications; will ensure that all agency partnership agreements identify an agency's critical applications; and will require State agency management approval when systems are added to, removed from, or reclassified on the Red Card. In addition, DTMB is assisting State agencies in understanding the importance of complete BCPs and DRPs through BCP/DR 101 training.

FINDING #3

Better coordination of plan preparation needed.

DTMB and State agencies did not always coordinate the preparation of DRPs and BCPs. Plans were not always created and did not adequately address recovery of both the business process and the information system.

DTMB Administrative Guide policy 1390 states that disaster recovery planning is part of business continuity planning. Also, according to NIST, system owners and others helping to prepare the plans need to work together to ensure that plans for restoring the system meet the needs of the business process.

We requested DRPs for 24 Red Card systems and infrastructure services and BCPs for the 29 associated business processes. We noted:

BCPs not prepared for all critical State business processes.

a. DTMB and State agencies did not prepare BCPs for any of the business processes supported by 10 (42%) of the 24 systems and infrastructure services, despite having identified these systems and services as critical to the State's operations. For 2 of these infrastructure services, DTMB was uncertain whether a BCP was necessary. For one additional system that supported 6 business processes, the agency created BCPs for only 5 of those processes. DRPs for systems that do not have corresponding BCPs were likely prepared without coordination with the agency's business continuity planning team, making it more difficult to ensure that business needs would be met.

b. State agencies did not identify the critical systems supporting the business processes for 3 (17%) of the 18 BCPs obtained, which may result in inadequately documented procedures for resuming operations if the systems are unavailable.

c. DTMB and State agencies did not document recovery times requested by the business owners in all DRPs. Recovery time objectives were not documented in 6 (38%) of the 16 application DRPs and 8 (42%) of the 19 hardware DRPs. In addition, recovery point objectives were not documented in 8 (50%) of the 16 application DRPs and 10 (53%) of the 19 hardware DRPs. If agency needs are not considered when DRPs are prepared, processes may not be restored timely and effectively.

DTMB has assigned only five staff to coordinate disaster recovery planning and one staff to coordinate business continuity planning for the State's approximately 1,700 IT applications, with limited coordination among the staff. Also, State agencies may fund projects that they consider to be a higher priority rather than fund disaster recovery and business continuity planning.

RECOMMENDATION

We recommend that DTMB and State agencies coordinate the preparation of DRPs and BCPs to help ensure that plans exist and contain the information needed to be effective in a disaster.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. In 2016, DTMB began a department-wide initiative to address existing internal control weaknesses in the State's information technology operations, referred to as the Material Internal Control Weaknesses Remediation and Accountability Program (MICWRAP). As part of this initiative, the department has now completed or substantially completed more than 80% of the DRPs for DTMB's 34 Red Card applications. Also, from this effort, DRPs for 75% of other departments' Red Card applications have been completed or substantially completed. DTMB will continue to assist State agencies in completing a business impact analysis to identify their critical, non-Red Card, applications and coordinate the preparation of remaining DRPs and BCPs. DTMB will also assist State agencies in understanding the importance of complete BCPs and DRPs through BCP/DR 101 training. In addition, DTMB will ensure there is adequate staffing available in the event of an emergency.

FINDING #4

DTMB did not implement a review process to ensure that DRPs and BCPs contained the necessary elements for effective disaster recovery.

DRPs and BCPs should be reviewed for completeness.

FISCAM recommends that plans be reviewed and updated at least annually. The SANS Institute* also recommends that plans be maintained by a business continuity coordinator or a disaster recovery coordinator who periodically reviews and distributes the plans to the owners to ensure that the plans are updated.

Critical elements omitted from DRPs and BCPs.

LDRPS tracks the completion status of each DRP and BCP stored in it. LDRPS calculates the completion percentage of each plan based on the number of sections the preparer has marked complete. The DR team distributes an LDRPS status report to DTMB managers monthly to remind them of the status of their plans. The following table summarizes the status of the DRPs for Red Card systems and for all BCPs stored in LDRPS as of October 1, 2015:

	Type of Plans in LDRPS		
	Application DRPs	Hardware DRPs	BCPs
Percentage completed:			
0%	6 (7%)	5 (6%)	31 (23%)
1% - 25%	11 (13%)	7 (8%)	12 (9%)
26% - 50%	14 (17%)	19 (23%)	7 (5%)
51% - 75%	16 (19%)	26 (31%)	6 (5%)
76% - 99%	15 (18%)	19 (23%)	13 (10%)
100%	22 (26%)	8 (10%)	63 (48%)
Total	84	84	132
Plans modified (including completing the plan) during last three months:			
Yes	12 (14%)	21 (25%)	4 (3%)
No	72 (86%)	63 (75%)	128 (97%)
Total	84	84	132

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

We reviewed DRPs for 24 of the 84 Red Card systems and infrastructure services. Our review included 16 application DRPs, 19 hardware DRPs, 5 vendor DRPs, 18 BCPs, and BCPs for the State's 3 hosting centers. We noted:

a. DTMB and State agencies did not document all necessary elements in the DRPs and BCPs, as noted below:

Missing Element	Application DRPs (16)	Hardware DRPs (19)	Vendor DRPs (5)	BCPs (18)
Annual review	14 (88%)	15 (79%)	4 (80%)	11 (61%)
Management approval	15 (94%)	18 (95%)	4 (80%)	15 (83%)
Annual testing	15 (94%)	17 (89%)	4 (80%)	14 (78%)
Requested recovery time objectives	6 (38%)	8 (42%)	2 (40%)	N/A
Requested recovery point objectives	8 (50%)	10 (53%)	3 (60%)	N/A
Detailed restoration procedures	13 (81%)	11 (58%)	0 (0%)	N/A
Business resumption procedures	N/A	N/A	N/A	8 (44%)
Prioritized order for recovering IT system components	11 (69%)	15 (79%)	1 (20%)	N/A
Defined criteria for activating the plan	7 (44%)	3 (16%)	1 (20%)	1 (6%)
Documented assumptions for creating the plan	5 (31%)	3 (16%)	1 (20%)	N/A
Business impact of the system	12 (75%)	15 (79%)	4 (80%)	N/A
System description	3 (19%)	7 (37%)	3 (60%)	N/A
Hardware configurations	N/A	9 (47%)	N/A	N/A
Up-to-date list of servers	N/A	4 (21%)	N/A	N/A
Up-to-date list of individuals involved in the recovery process	11 (69%)	19 (100%)	0 (0%)	1 (6%)
Procedures to alert individuals during business hours	7 (44%)	7 (37%)	1 (20%)	4 (22%)
Procedures to alert individuals during non-business hours	7 (44%)	19 (100%)	1 (20%)	6 (33%)
Resources required to support business continuity during a disaster	N/A	N/A	N/A	3 (17%)
Applications needed to support normal business operations identified	N/A	N/A	N/A	4 (22%)
Potential scenarios that could cause a disruptive incident	N/A	N/A	N/A	7 (39%)

N/A – Not applicable (i.e., element not necessary for this type of plan).

Without these important elements, DRPs and BCPs may not be effective and could result in delays in restoring critical systems and business processes. The summary of elements missing from DRP and BCP testing, presented as supplemental information, identifies the importance of each element.

b. DTMB did not always include critical elements in BCPs for the State's 3 hosting centers. Although hosting center BCPs did include 16 of the 19 elements tested, DTMB did not:

(1) Review the BCP for 1 (33%) of the 3 hosting centers to ensure that it contained the necessary elements and was up to date.

(2) Test the BCP for 1 (33%) of the 3 hosting centers.

Testing can identify weaknesses in the plan and help ensure that the plan will work as intended in a disaster.

(3) Document DTMB division director approval of the BCP for any of the 3 hosting centers.

Management should understand the impact from the loss of data. Obtaining management support and approval helps to ensure that adequate resources are devoted to emergency planning, training, and testing.

DTMB and several State agencies informed us that the incomplete plans noted in parts a. and b. resulted from a lack of guidance, time, staff, and funding and from difficulties using LDRPS. DTMB policy requires annual testing of DRPs and BCPs. However, DTMB did not provide guidance on required testing and the extent to which the testing of DRPs and BCPs should be performed together.

RECOMMENDATION

We recommend that DTMB implement a review process to ensure that DRPs and BCPs contain the necessary elements for effective disaster recovery.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and, as part of the MICWRAP initiative, has implemented a review process to ensure that DRPs and BCPs contain all the necessary elements for effective disaster recovery. In addition, DTMB has revised DRP and BCP training to help ensure all necessary elements are documented and contained in the DRPs and BCPs. DTMB has also created a training schedule for providing BCP/DR 101 training to State agencies.

FINDING #5

More DR servers needed.

DTMB did not ensure that DR servers were in place for all Red Card systems. An incident at a hosting center could significantly delay recovery time for these critical systems if DR servers are not in place.

FISCAM states that entities should have DR servers for critical systems.

We tested 20 of the 74 State-hosted Red Card systems and noted that 3 (15%) of the 20 systems did not have DR servers.

DR servers are not required by DTMB policy.

DTMB policy does not require that DR servers be used for Red Card systems. Instead, DTMB Agency Services works with State agencies to determine if the server is needed. However, some agencies may not have funding available for separate DR servers or may choose to allocate available funding to other priorities.

RECOMMENDATION

We recommend that DTMB ensure that DR servers are in place for all Red Card systems.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will work with State agencies to ensure that DR servers are in place for all Red Card systems. DTMB will assist State agencies in completing a business impact analysis to identify their critical applications; coordinate the preparation of DRPs and BCPs; and communicate the importance of funding DR servers.

FINDING #6

Improvements needed to LDRPS access.

DTMB, in conjunction with State agencies, did not grant and maintain appropriate access to the DRPs stored in LDRPS. Proper access would allow DTMB and agency staff to ensure that plans can be updated and retrieved in a timely manner to expedite system recovery.

According to NIST, recovery plans should be provided to recovery personnel. Also, access should be restricted because of confidential information contained in the plans. In addition, DTMB Administrative Guide policy 1335 states that agencies should develop a formal process to manage user access to the State's IT resources.

Recovery staff did not have necessary access to LDRPS to ensure plans were updated and tested.

We reviewed access to the 16 application, 19 hardware, and 1 vendor DRPs stored in LDRPS as of October 2015. DTMB, in conjunction with State agencies, did not grant access to:

a. 5 (31%) of the 16 application DRPs stored in LDRPS to anyone within DTMB Agency Services or the State agencies.

b. 16 (84%) of the 19 hardware DRPs in LDRPS to anyone within DTMB Technical Services.

   After bringing this to management's attention, DTMB provided one of its Technical Services employees with access to the plans.

The Emergency Management Coordinator and the five DR team employees had access to all of the DRPs in LDRPS, including the DRPs mentioned in parts a. and b. above. In a disaster, the Emergency Management Coordinator and DR team could provide the plans to the other DTMB and agency staff who will be restoring the systems. However, relying on six employees to distribute plans rather than providing direct access to employees responsible for recovering systems after a disaster would likely delay recovery efforts. Without appropriate access to the DRPs, DTMB and the agencies cannot ensure that their plans are reviewed, updated, and tested.

DTMB and agency staff did not have access to the plans because DTMB had not defined which individuals within DTMB and the agencies should be granted access to LDRPS and the DR team was not always aware of which users should have access to each plan. Also, agencies are responsible for requesting access to the plans, but they did not request access.

RECOMMENDATION

We recommend that DTMB, in conjunction with State agencies, grant and maintain appropriate access to the DRPs stored in LDRPS.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will work with State agencies to grant and maintain appropriate access to the DRPs stored in LDRPS. DTMB will implement a periodic review of DR/BCP access.

FINDING #7

DTMB and State agencies did not fully utilize a central repository and backup storage location for DRPs and BCPs to ensure that plans are readily available in the event of a disaster.

Improved storage of DRPs and BCPs needed.

DTMB Administrative Guide policy 1390 states that DTMB is responsible for maintaining a highly available repository for agencies to store DRPs and BCPs and that State agencies are responsible for ensuring that their DRPs and BCPs are stored within the repository. In addition, NIST recommends that plans be distributed to recovery personnel for storage and that copies of the plans be stored in a backup location to ensure that they are in good condition if the primary copies are inaccessible because of the disaster.

DTMB uses LDRPS as its central repository for DRPs and BCPs.

DRPs and BCPs not always stored in LDRPS and a backup location.

We assessed the location of DRPs and BCPs for 24 Red Card systems and infrastructure services, including 16 application DRPs, 19 hardware DRPs, 5 vendor DRPs, and 18 BCPs. DTMB and State agencies did not store DRPs and BCPs:

a. In LDRPS, as required by DTMB policy.

   DRPs for 4 (80%) of the 5 vendor-managed or vendor-hosted systems and 15 (83%) of the 18 BCPs were not stored in LDRPS.

b. In a backup location.

   Some plans were only stored in a single location, such as on a network shared drive with no hard-copy version. NIST recommends storing plans in multiple locations in the event the primary copies are unavailable because of the disaster.

DTMB and agency staff informed us that some plans were not stored in LDRPS because the system is difficult to use. One agency incorrectly believed that storing plans on a network drive was acceptable.

RECOMMENDATION

We recommend that DTMB and State agencies fully utilize a central repository and backup storage location for DRPs and BCPs.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB's IT Continuity of Business Planning Standard 1340.070.002 now states that all plans, regardless of where of the applications are housed, must be in the State's central repository. DTMB will work with State agencies to ensure that DRPs and BCPs utilize LDRPS as the State's central repository.

FINDING #8

Improved version control needed.

DTMB and State agencies did not implement effective version control for DRPs and BCPs. As a result, DTMB and agency staff were sometimes unaware of the existence and location of the current version of the DRPs and BCPs, increasing the risk of updating or using an incorrect version of the plans.

NIST recommends that entities maintain version control over DRPs and BCPs, which could be achieved by using a central storage system, to ensure that old versions are not in circulation. NIST also recommends that copies of plans be provided to recovery personnel for storage.

We requested DRPs for 24 Red Card systems and infrastructure services and BCPs for the 29 associated business processes. Our review included 16 application DRPs, 19 hardware DRPs, 5 vendor DRPs, and 18 BCPs. We identified instances in which the lack of version control may result in DTMB being unable to recover systems within the necessary time frames. For example:

a. A DTMB division manager for one infrastructure service was unaware of whether DRPs or BCPs existed for that service. After 22 business days, the manager provided us with the application and hardware DRPs; however, the plans were missing critical information needed to restore the service and no BCP existed for this service.

Multiple versions of some DRPs and BCPs exist, making it difficult for staff to know which version should be used.

b. One agency and its DTMB Agency Services manager had different versions of the DRP for a system. However, Agency Services determined that neither plan would be used for disaster recovery and provided us with a third version of the plan. Agency Services took 18 business days to identify and provide the correct application and hardware DRPs for the system.

c. DTMB had to contact the vendor to obtain copies of the DRP for one system. DTMB provided the plan to us 24 business days after our initial request.

d. One agency provided DRPs for one system and a few days later provided a different DRP for the same system. Although the agency was able to confirm the correct plan within 8 business days, having multiple versions of DRPs could hinder recovery efforts if those involved in the process are unaware of the other plans or are not sure which plan should be used.

Although an actual disaster would likely expedite DTMB and the agencies' retrieval of the plans, DTMB should establish a process to ensure that only current versions of DRPs and BCPs are available to staff and that staff know where the current versions are stored. Storing all DRPs and BCPs in a central repository may improve version control.

RECOMMENDATION

We recommend that DTMB and State agencies implement effective version control for DRPs and BCPs.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB will work with State agencies to ensure that DRPs and BCPs utilize LDRPS, as the State's central repository, which will enforce version control for DRPs and BCPs.

SUPPLEMENTAL INFORMATION

UNAUDITED

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

Summary of Elements Missing From DRP and BCP Testing

Missing Element	Purpose/Effect
Annual review	Ensures that plan information, such as server names and key individuals, is still accurate and complete.
Management approval	Helps ensure that adequate resources are devoted to emergency planning, training, and testing.
Annual testing	Helps ensure that plans will function as intended and meet the needs of the agency; also helps identify weaknesses in the plan.
Requested recovery time objectives	Help ensure that sufficient recovery resources are assigned.
Requested recovery point objectives	Help ensure that sufficient recovery resources are assigned.
Detailed restoration procedures	Ensure that systems and business processes can be restored correctly and timely, including steps for validating system functionality and alerting appropriate individuals.
Business resumption procedures	Ensure that systems and business processes can be restored correctly and timely.
Prioritized order for recovering IT system components	Ensures that recovery is done in an efficient sequence.
Defined criteria for activating the plan	Helps ensure that plan is activated only during appropriate scenarios.
Documented assumptions for creating the plan	Identify dependencies on other IT resources and situations that the plan does not cover.
Business impact of the system	Helps identify critical processes and ensure that the most critical functions are restored first in a major disaster.
System description	Helps identify why the system is important and who it is important for.
DTMB's listing of the State's hardware configurations	Ensures that hardware is recovered using State-recommended security configurations.
Up-to-date list of servers	Ensures that servers can be located in the event of a disaster.
Up-to-date list of individuals involved in the recovery process	Helps ensure that responsible individuals can be reached promptly during a disaster.
Procedures to alert individuals during business hours	Help ensure that responsible individuals can be reached during a disaster.
Procedures to alert individuals during non-business hours	Help ensure that responsible individuals can be reached during a disaster.
Resources required to support business continuity during a disaster	Ensure that resources needed to resume business operations, such as alternate work facilities, staff, IT systems, and computers, are available.
Applications needed to support normal business operations are identified.	Ensure that all critical applications have been identified and properly planned for.
Scenarios that could cause a disruptive incident	Help assess the likelihood of activating the plan and allow for better disaster recovery and business continuity planning.

Source: Prepared by the Office of the Auditor General from information obtained from NIST, FISCAM, and Control Objectives for Information and Related Technology (COBIT).

DESCRIPTION

The State's business continuity planning structure is composed of multiple layers:

- Statewide plan - The State's Emergency Management Center (SEMC) manages continuity planning at the Statewide level and is responsible for the preparation and maintenance of the continuity of government plan (COG).

- Department plans - Each State department prepares a continuity of operations plan* (COOP) to address business continuity for its department.

- Business process plans - Each agency that operates essential functions prepares a BCP for each critical process to document the steps for resuming normal operations during and after a disaster.

- IT system plans - DRPs are created for IT systems that support critical business processes, which document all information needed to recover the systems. Systems located in the State's 3 hosting centers typically have two separate DRPs, one for the application recovery process and another for recovering the hardware.

Various DTMB teams are involved in the preparation of DRPs and BCPs:

- DTMB Data Center Operations DR team:
    - Manages LDRPS, which is the State's repository for creating and maintaining DRPs and BCPs.
    - Creates templates for application and hardware DRPs in LDRPS and adds the basic information to the plans from the DTMB-208 form.
    - Assists DTMB Agency Services, DTMB Technical Services, and agency staff in completing DRPs upon request.
- DTMB Agency Services staff, in conjunction with agency staff, complete the application DRP.
- DTMB Technical Services staff complete the hardware DRP.

The Emergency Management Coordinator, within the DTMB Office of Infrastructure Protection, is available to assist agencies in preparing BCPs for their critical business processes.

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

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the State's processes for developing and maintaining DRPs and BCPs. 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 conclusion based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion based on our audit objective.

Our audit does not include business continuity planning for business processes that do not rely on critical information systems. Our audit includes business continuity planning at the business process level and not at the department or Statewide level.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2013 through January 31, 2016.

METHODOLOGY

We conducted a preliminary survey of the State's processes for creating and maintaining DRPs and BCPs to formulate a basis for defining our audit objective and scope. During our preliminary survey, we:

- Reviewed policies and procedures and interviewed DTMB and State agency management and staff to obtain an understanding of disaster recovery and business continuity planning.
- Obtained an understanding of DTMB's processes to create DRPs and BCPs in LDRPS and grant user access to LDRPS.
- Obtained and reviewed example DRPs and BCPs.

OBJECTIVE

To assess the effectiveness of the State's efforts to develop and maintain DRPs and BCPs for State of Michigan business functions supported by IT systems.

To accomplish this objective, we:

- Judgmentally selected 24 critical systems and infrastructure services from the DTMB Red Card and

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

reviewed DRPs and BCPs for the business processes that rely on these systems and services.

- Gained an understanding of the process to add systems and infrastructure services to the Red Card and compared the process with best practices.

- Reviewed the completeness and accuracy of the Red Card.

- Evaluated the definition of critical systems for the Red Card and compared the systems listed with systems on other critical systems lists to determine the accuracy and completeness of the Red Card.

- Reviewed user access to LDRPS.

- Evaluated the location of production and DR servers to ensure existence of the DR servers and appropriate physical separation from the production servers.

- Inquired of the State agencies about their opinion of disaster recovery and business continuity planning.

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 audits on an exception basis.

CONFIDENTIAL AND SENSITIVE INFORMATION

Because of the confidentiality of certain findings, we summarized our testing results for presentation in those findings and provided the detailed results to DTMB management.

AGENCY RESPONSES

Our audit report contains 8 findings and 8 corresponding recommendations. DTMB's preliminary response indicates that it agrees with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion at the end of our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

SUPPLEMENTAL INFORMATION

Our audit report includes supplemental information. Our audit was not directed toward expressing a conclusion on this information.

GLOSSARY OF ABBREVIATIONS AND TERMS

Active Directory	Microsoft Windows operating system software that provides an integrated and single sign-on system using a central repository containing user IDs and user permissions that allow centralized management of users and their security.
business continuity	An ongoing process to ensure that steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.
business continuity plan (BCP)	Documentation of a predetermined set of instructions or procedures, at the business process level, that describes how an organization's mission and business processes will be sustained during and after a significant disruption to operations.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over information technology.
continuity of operations plan (COOP)	A predetermined set of instructions or procedures, at the department level, that describes how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.
disaster (as related to disaster recovery plans)	A sudden, unplanned catastrophic event causing unacceptable damage or loss that compromises an organization's ability to provide critical functions or services for an unacceptable amount of time.
disaster recovery (DR)	The technical aspect of business continuity that 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 written plan for recovering information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
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.*
IT	information technology.
Living Disaster Recovery Planning System (LDRPS)	An IT system used by DTMB to create, store, and maintain the State's DRPs and BCPs.
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.
MICWRAP	Material Internal Control Weaknesses Remediation and Accountability Program.
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 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.
recovery point objective	The point in time by which data must be recovered after an outage.
recovery time objective	The length of time an information system can be in the recovery phase before negatively impacting an organization's mission or business processes.
Red Card	A document maintained by DTMB that identifies IT services and applications associated with State agency-identified critical business functions.

reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.
SANS Institute	A research and education organization that develops, maintains, and makes available at no cost research documents about various aspects of information security. The SANS Institute also offers computer security training and certification.

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