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