Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump

Making government work better

Official Audit Report – Issued February 1, 2018

Merit Rating Board

For the period July 1, 2014 through June 30, 2016

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

February 1, 2018

Mr. Thomas Bowes, Director
Merit Rating Board
PO Box 55889
Boston, MA 02205-5889

Dear Mr. Bowes:

I am pleased to provide this performance audit of the Merit Rating Board. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2014 through June 30, 2016. My audit staff discussed the contents of this report with management of the agency, whose comments are reflected in this report.

I would also like to express my appreciation to the Merit Rating Board for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Stephanie Pollack, Secretary and Chief Executive Officer, Massachusetts Department of Transportation

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ALARS	Automated License and Registration System
BCP	business continuity plan
COBIT	Control Objectives for Information and Related Technologies
DR	disaster recovery
FTP	File Transfer Protocol
HR	human resources
ISP	information security program
IT	information technology
ITGC	information technology general control
MassDOT	Massachusetts Department of Transportation
MassIT	Massachusetts Office of Information Technology
MRB	Merit Rating Board
NIST	National Institute of Standards and Technology
PII	personally identifiable information
RMV	Registry of Motor Vehicles
OSA	Office of the State Auditor

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted an audit to review and evaluate controls over selected information technology (IT) operations and activities of the Merit Rating Board (MRB) for the period July 1, 2014 through June 30, 2016.

In this performance audit, we reviewed certain IT controls over MRB mission-critical applications related to logical access security; change management (monitoring, documenting, and approving modifications to an agency's IT system); personally identifiable information (PII); and business continuity planning and disaster recovery (DR).

Our audit of MRB identified an issue that has been omitted from this report in accordance with Exemption (n) of the Commonwealth's public-records law (Section 7[26] of Chapter 4 of the General Laws), which allows for the withholding of certain records, including security measures or any other records related to cybersecurity or other infrastructure, if their disclosure is likely to jeopardize public safety or cybersecurity.

In accordance with Sections 7.39–7.43 of the Government Accountability Office's Government Auditing Standards, as well as OSA policies, for reporting confidential and sensitive information, we have given a separate, full report to MRB, which will be responsible for acting on our recommendations.

Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1a **Page 9**	MRB did not have policies and procedures in place to remove access rights to its Automated License and Registration System (ALARS) when employees were terminated.
Finding 1b **Page 10**	MRB did not review employee access rights to ALARS quarterly.

Recommendations **Page 10**	1. MRB should define a specific timeframe to revoke terminated employees' access to ALARS. It should also develop its own logical access security policies and procedures to supplement the Massachusetts Department of Transportation's (MassDOT's) information security program. 2. MRB should develop and implement a process to review the access rights for all ALARS user accounts and work with the Information Technology Division of MassDOT (MassDOT IT) to obtain the information necessary to perform this activity. MRB should include access rights in its monthly ALARS reports to managers, or MRB could establish a process of review at least quarterly to ensure that users' access rights are limited to their individual job requirements.
Finding 2a **Page 11**	MRB did not have policies and procedures to classify data and maintain a data inventory.
Finding 2b **Page 12**	Employees did not receive IT security training before they received access to ALARS.
Recommendations **Page 13**	1. MRB should consult with MassDOT to develop policies and procedures to classify and inventory its data in case of loss or corruption. In addition, a periodic review should be put in place to ensure that this procedure occurs regularly. 2. MRB should ensure that all new employees receive security awareness training during the onboarding process, before they receive access to MRB systems.
Finding 3a **Page 13**	MRB did not have a business continuity plan (BCP).
Finding 3b **Page 14**	MRB did not test a DR plan for fiscal years 2015 and 2016.
Finding 3c **Page 14**	MRB did not have backup policies and procedures for its internal FTP server.
Recommendations **Page 15**	1. MRB should work with MassDOT IT to develop, document, and implement a BCP that includes MRB operations. 2. MRB should consult with MassDOT to perform a DR test for all critical IT assets (such as data, equipment, IT services, and IT personnel) to ensure that suitable alternative procedures exist in case disruptions occur. The DR test should be performed annually to minimize the duration of any disruption to MRB operations. 3. MRB should consult with MassDOT to document, develop, and implement backup procedures for its servers. These procedures should ensure that full offsite backups are performed and maintained regularly.

OVERVIEW OF AUDITED ENTITY

The Merit Rating Board (MRB) was established in 1976 in accordance with Section 57A of Chapter 6C of the Massachusetts General Laws and is a subdivision of the Massachusetts Department of Transportation's (MassDOT's) Registry of Motor Vehicles (RMV). MRB is managed by a director appointed by the Registrar of Motor Vehicles, the Commissioner of Insurance, and the Attorney General. Its primary mission is to maintain and update driving records and report driving record information to Massachusetts auto insurers and other transportation and public-safety government agencies. More specifically, its day-to-day operations include the following:

- receiving insurance claims from insurers and applying each claim incident to the individual's driving record
- processing requests for driving history information from insurers, applying each inquiry to the individual's driving record, and returning a response to the insurer
- receiving out-of-state driving records from insurers and applying each out-of-state incident to the individual's driving record
- designing and operating the software underpinning the Safe Driver Insurance Program,[1] as well as the software that manages electronic data transfers between MRB and courts, law enforcement agencies, the Division of Insurance's Board of Appeals, financial institutions, and automobile insurers

MRB's mission-critical and essential application system is the Automated License and Registration System (ALARS). According to the RMV's Uninsured Motorist System User Manual, ALARS consists of multiple components, including licensing, registration, titles, suspensions, accident records, inspection maintenance, non-renewals, policies, and MRB information. MRB information includes motor vehicle violation citations (civil and criminal), at-fault accident claim records, comprehensive claim records, and out-of-state incidents. The intended users of ALARS include MRB's staff, Trial Court administrators, the Division of Insurance's Board of Appeals, and insurance companies and agents.

A division of MassDOT, MRB depends on MassDOT for its information technology needs (such as installing its workstations and software upgrades) and human-resource functions.

[1] The Safe Driver Insurance Program is a program administered by the RMV that tracks an individual's driving record and gives automobile insurers a framework so that they can charge individual customers additional surcharges on insurance premiums depending on their driving records.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of the Merit Rating Board (MRB) for the period July 1, 2014 through June 30, 2016.

Information technology general controls (ITGCs) are a subset of internal controls within a performance audit that are applied to every information technology (IT) system an organization relies on and to the IT staff members who administer those systems. They provide management and stakeholders with assurance regarding the reliability of data and information systems. ITGCs are meant to ensure the confidentiality, integrity, and availability of systems, programs, data files, and computer operations in an organization.

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.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and, if applicable, where each objective is discussed in the audit findings.

Objective	Conclusion
1. Has MRB designed and effectively implemented certain ITGCs to support its mission-critical and essential application systems?	
a. Has MRB designed and effectively implemented logical access security controls, such as background checks for new users; approval processes for new, transferred, and terminated user accounts; and password security, to support its mission-critical application systems?	**No; see Findings 1a and 1b**
b. Has MRB designed and effectively implemented change-management controls to support its mission-critical and essential application systems?	**Yes**

Objective	Conclusion
c. Has MRB designed and effectively implemented personally identifiable information (PII) controls, such as new-user Acknowledgement Forms and new-employee training, to support its mission-critical application systems, and has it established confidentiality agreements with contractors, vendors, and other third parties?	**No; see Findings 2a and 2b**
d. Has MRB designed and effectively implemented a business continuity plan (BCP) and disaster recovery (DR) controls, such as established policies and procedures and annual testing, to support its mission-critical and essential application systems?	**No; see Findings 3a, 3b, and 3c**

We conducted this performance audit using criteria from the Massachusetts Department of Transportation's (MassDOT's) information security program (ISP), which documents how MassDOT agencies should keep data secure and reduce the risk of unauthorized disclosure. If MassDOT's ISP was deficient in a certain area, we relied on industry standards established by (1) the Information Systems Audit and Control Association in its document Control Objectives for Information and Related Technologies (COBIT) 4.2, (2) the National Institute of Standards and Technology, and (3) the Massachusetts Office of Information Technology (MassIT). Although MRB is not required to follow these industry standards, we believe they represent IT-industry best practices for ITGCs. For example, the purpose of COBIT is to provide management and business-process owners with an IT governance model that helps them deliver value from IT and understand and manage the risks associated with IT. According to the Information Systems Audit and Control Association's website,

> *COBIT helps bridge the gaps amongst business requirements, control needs and technical issues. It is a control model to meet the needs of IT governance and ensure the integrity of information and information systems.*

We gained an understanding of the internal controls we deemed significant to our audit objectives through interviews and observations, and we evaluated the design of MRB's logical access security, change management, and PII controls, as well as whether it had a BCP and DR plan.

To achieve our objectives, we performed the following audit procedures:

- We assessed logical access security controls, such as background checks for new users; approval processes for new, transferred, and terminated user accounts; and password security during the audit period. Specifically, we performed the following procedures:

  - We requested and verified documentation of the Criminal Offender Record Information checks for all four new employees who were hired during the audit period to ensure that these employees had been properly screened before gaining access to the Automated License and Registration System (ALARS).

  - We reviewed all four new users' access approvals by verifying their managers' signatures and dates to ensure that their access to ALARS had been properly approved.

  - We observed the MassDOT Human Resources (HR) Compensation Management System database administrator building a Structured Query Language query to obtain the MRB employee list. The database administrator sorted the data, exported the data to Excel, and saved the data on a USB drive provided by OSA.

  - We also noted that no employees transferred during the audit period, so we did not request documentation to determine whether the access rights of transferred employees had been adjusted properly to reflect their new roles.

  - We compared the employee termination list provided by HR to an ALARS user-account termination list to determine whether the accounts of all nine employees who were terminated during the audit period had been removed upon termination.

  - We interviewed the IT security officer to determine whether user accounts and account access rights to ALARS were reviewed periodically. We reviewed the accounts of all four new users and all nine terminated employees to verify their access status.

  - We selected a nonstatistical judgmental sample of emails to determine whether user accounts and account access rights to ALARS were reviewed periodically. Since the IT security officer sends quarterly emails to MRB management, we selected emails from six out of eight quarters for review. Because our sampling was nonstatistical, we did not project the results of our audit tests to the total populations in the areas we reviewed.

  - We requested password parameters for ALARS and observed the testing of those parameters to ensure that the requirements set by MassDOT were followed. To achieve this, we observed while the ALARS security officer tested the password parameters.

- We assessed MRB's controls to determine whether change management (monitoring, documenting, and approving modifications to the IT system) was administered adequately. Specifically, we performed the following procedures:

  - We interviewed the MRB IT consultant and the customer-engagement manager for the MassDOT Information Technology Division (MassDOT IT) to obtain an understanding of how the testing and production environments functioned. We also observed the MRB IT consultant logging into the testing and production servers to verify that production and testing environments were separate.

  - We reviewed the MassDOT IT flowchart for the project proposal process and the change-management policy to gain an understanding of the steps and requirements that MRB follows at different phases of IT project change management.

  - We reviewed 100% of the management signoffs of two change tickets (open issues discovered during testing of the two File Transfer Protocol [FTP] server replacement projects) that occurred during our audit period.

- We assessed MRB's controls to determine whether protected information was properly safeguarded. The controls included new-user Acknowledgement Forms; new-employee training; and confidentiality agreements with contractors, vendors, and other third parties. Specifically, we performed the following procedures:

  - We interviewed MassDOT's HR managers to obtain an understanding of MRB's onboarding process for new employees and to verify that all four new employees signed Acknowledgement Forms before gaining access to MRB's protected information.

  - We reviewed training documentation provided by MassDOT's HR manager and interim training manager to determine whether all four new employees had completed security training before working with protected information.

  - We reviewed confidentiality agreements for all four new employees to verify that they had all signed the agreements before working with protected information.

  - We interviewed managers from MassDOT and MRB to determine whether documentation regarding data classification and data inventory existed.

  - We observed the MRB IT consultant logging into the server administrative account and obtained screenshots of internal FTP server security controls, such as login identification and password parameters.

  - We interviewed MRB management and requested the MassDOT Shared Vendor Assessment document and the Service Organization Controls Reports to determine the security controls of the service provider's[2] FTP server.

- We assessed MRB's controls to determine whether BCP and DR processes, such as established policies and procedures and annual testing, were in place and properly managed to support its mission-critical and essential application systems. Specifically, we performed the following procedures:

  - We interviewed MassDOT IT managers and MRB IT personnel and obtained documentation related to the 2014 MassIT DR test to determine whether the DR test was performed annually. This documentation consisted of a backup and recovery test schedule for June 2014 created by MassIT for ALARS and various other state systems.

  - We assessed the reliability of MRB data in ALARS and the HR system. Specifically, we reviewed existing information and interviewed knowledgeable staff members about the data. In addition, we performed validity and integrity tests on all data, including (1) testing for missing data, (2) scanning for duplicate records, (3) testing for values outside a

[2] Microsoft is the service provider that operates the FTP server, which insurance companies use to transmit data and information to MRB.

designated range, and (4) looking for dates outside specific time periods. Based on our analysis, we determined that the data were sufficiently reliable for the purposes of this audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Merit Rating Board had inadequate logical access controls for its Automated License and Registration System.

The Merit Rating Board (MRB) did not have adequate logical access controls for its Automated License and Registration System (ALARS). Without such controls, there is a risk that data in the system may be corrupted or manipulated by former employees who did not have their access removed upon termination. Furthermore, without proper and regular review of access rights, MRB increases the risk that a terminated employee's account could be compromised and used to manipulate data in ALARS.

a. MRB did not have policies and procedures in place to remove access rights to ALARS when employees were terminated.

Six of the nine employees terminated during our audit period did not have their access to ALARS revoked immediately upon termination of employment. One terminated employee did not have his access revoked for 140 days, and five others did not have their access revoked for more than 3 days. This increases the risk of terminated employees improperly accessing and/or altering personal information in ALARS such as names, addresses, driver's license numbers, dates of birth, and driving records.

Authoritative Guidance

The Massachusetts Office of Information Technology (MassIT) requires all executive department agencies and any agency or third party that connects to the Commonwealth's wide-area network, Massachusetts Access to Government Networks, to comply with its Enterprise Information Security Policy, which states,

> *Agencies are required to ensure that employees, contractors and third party users understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to reduce the risk of unauthorized access, use or modification of IT Resources (theft, fraud or misuse of facilities), including . . .*
>
> - ***Removal of access rights upon termination of employment.*** [Emphasis added.]

Reasons for Noncompliance

The Massachusetts Department of Transportation's (MassDOT's) information security program (ISP) establishes a timeframe to revoke access for terminated employees who handle electronic payments, but does not define a specific timeframe for the revocation of access for other employees, such as those who work at MRB. In addition, MRB did not have its own logical access security policies and procedures to supplement MassDOT's ISP.

b. MRB did not review employee access rights to ALARS quarterly.

MRB did not establish a process for reviewing employee access rights quarterly, so there was no verification that the user accounts were limited to the fewest privileges necessary for employees' job duties. This increases the risk of some employees having access to and/or altering personal information in ALARS beyond what their job duties require.

Authoritative Guidance

MassDOT's ISP states,

> *A **quarterly** (every three [3] months) review of all accounts, including remote access accounts, will be conducted to ensure that the accounts are still necessary and **access rights are limited to the least privileges to meet business need**.* [Emphasis added.]

Reasons for Noncompliance

Managers monitored ALARS users monthly but were not given reports at least quarterly that identified access rights granted to each user. Without this information, they could not properly review and approve access rights for all employees.

Recommendations

1. MRB should define a specific timeframe to revoke terminated employees' access to ALARS. It should also develop its own logical access security policies and procedures to supplement MassDOT's ISP.
2. MRB should develop and implement a process to review the access rights for all ALARS user accounts and work with the MassDOT Information Technology Division (MassDOT IT) to obtain the information necessary to perform this activity. MRB should include access rights in its monthly ALARS reports to managers, or MRB could establish a process of review at least quarterly to ensure that users' access rights are limited to their individual job requirements.

Auditee's Response

> *The Merit Rating Board does not have any control over who has access to ALARS. Merit Rating Board only makes requests for access. Merit Rating Board is totally dependent on MASSDOT IT for establishing and maintaining access to ALARS for the Merit Rating Board. . . .*
>
> *The recommendation that the Merit Rating Board establish better review procedures for checking on ALARS for terminated employees is reasonable.*

Auditor's Reply

As noted above, MRB did not have policies and procedures in place to remove access rights from ALARS when employees were terminated. Although MassDOT IT may be responsible for actually initiating and removing these access rights, MRB is responsible for establishing the access rights for its employees, monitoring its accounts, and asking MassDOT IT to modify or terminate these rights in a timely manner as necessary. Without such controls, there is a risk that data in the system may be corrupted or manipulated by former employees and that a terminated employee's account could be compromised and used to manipulate data in ALARS.

2. MRB had inadequate controls to process personally identifiable information.

MRB did not have adequate controls in place to process personally identifiable information (PII). MassIT and MassDOT both have guidelines in place for agencies and sub-agencies to follow, but MRB did not adhere to some of these guidelines. By not following these guidelines, MRB increases the risk that PII may be compromised and used inappropriately.

a. MRB did not have policies and procedures to classify data and maintain a data inventory.

We requested from MRB management a copy of policies and procedures related to data classification and the maintenance of a data inventory, but MRB did not have such policies and procedures. Without policies and procedures to guide the data classification and data inventory process, MRB is not aware of what data could be missing or lost.

Authoritative Guidance

MassIT's Enterprise IT Security Compliance Policy states,

> *Agencies must develop and implement uniform policies and standards that meet the compliance requirements associated with the sensitivity classification of their data as articulated in the Enterprise Information Security Standards: Data Classification.*

Furthermore, MassIT's Enterprise IT Asset and Risk Management Policy states,

> *Secretariats and their respective Agencies must maintain an* ***inventory of IT assets*** *which consist of physical IT assets (hardware, network devices, etc.) and logical IT assets (****data****, software, licensing, and applications).* [Emphasis added.]

Reasons for Noncompliance

MRB management told us that they were not aware that they were responsible for developing data classification and data inventory procedures. They instead assumed that MassDOT IT was responsible.

b. Employees did not receive information technology security training before they received access to ALARS.

In reviewing the training logs for four employees hired during the audit period (who included full-time employees, interns, and contractors), we found that three employees received access to ALARS even though they had not received security awareness training during the onboarding process. Insufficient security awareness may lead to user error and compromise the integrity and security of protected information in MRB systems.

Authoritative Guidance

Massachusetts Executive Order 504 states,

> *All agency heads, managers, supervisors, and employees (including contract employees) shall attend mandatory information security training within one year of the effective date of this Order. For future employees, such training shall be part of the standardized orientation provided* ***at the time they commence work****.* [Emphasis added.]

Reasons for Noncompliance

MassDOT's ISP did not define a required timeline for completing security awareness training.

Recommendations

1. MRB should consult with MassDOT to develop policies and procedures to classify and inventory its data in case of loss or corruption. In addition, a periodic review should be put in place to ensure that this procedure occurs regularly.

2. MRB should ensure that all new employees receive security awareness training during the onboarding process, before they receive access to MRB systems.

Auditee's Response

> *The Merit Rating Board has no control over data classification or data inventory. We are totally dependent on MASSDOT IT to control and maintain the ALARS database. These deficiencies in these policies and procedures will be directed towards MASSDOT IT. . . .*
>
> *The Merit Rating Board will work with MASSDOT IT for security training prior to employees receiving access to ALARS.*

Auditor's Reply

We acknowledge that it is MassDOT IT's responsibility to control and maintain the ALARS database. However, MRB also needs to work with MassDOT IT and provide it with the information necessary for MassDOT IT to effectively administer this process. This is why we recommend that MRB consult with MassDOT to develop policies and procedures to classify and inventory its data in case of loss or corruption.

Based on its response, MRB is taking some measures to address our concerns in this area.

3. MRB did not document and test a business continuity plan.

MRB lacked proper procedures for dealing with incidents that might compromise its ability to recover from disruptions to its operations or destruction of data that are vital to serving the citizens of the Commonwealth. Without proper procedures (such as regular backups of data) to safeguard the continuance of normal operations after a disaster, it may be difficult, if not impossible, for MRB to fulfill its mission.

a. MRB did not have a business continuity plan.

We interviewed MRB management and MassDOT IT staff members and found that MRB did not have a business continuity plan (BCP) that was documented, implemented, and up to date for all mission-critical objectives. This may cause MRB's critical operations to be disrupted in the event of a loss of data or systems.

Authoritative Guidance

MassIT's Enterprise Business Continuity for IT Management Policy states,

> *Agencies are required to develop, implement, test, and maintain a Business Continuity Plan (BCP) for all Information Technology Resources (ITR) that deliver or support core systems and services on behalf of the Commonwealth of Massachusetts.*

The minimum components set by MassIT for a BCP are standard incident response procedures, a disaster recovery (DR) plan, and a continuity-of-operations plan.

Reasons for Noncompliance

MRB management stated that MRB followed MassDOT's ISP instead of developing its own. MassDOT IT staff members could not provide a reason that no BCP had been developed.

b. MRB did not test a DR plan for fiscal years 2015 and 2016.

MRB did not perform a DR test for fiscal years 2015 and 2016 to assess its ability to sustain operations in the event of a business interruption. This increases the risk that the confidentiality, integrity, and availability of MRB information will be compromised.

Authoritative Guidance

According to MassIT's Enterprise Business Continuity for IT Management Policy,

> *Agencies are required to document, implement and* ***annually*** *test plans [including DR plans] including the testing of all appropriate security provisions to minimize impact to systems or processes from the effects of major failures of IT Resources or disasters.* [Emphasis added.]

Reasons for Noncompliance

MRB received an email from MassIT regarding the DR test for fiscal year 2015, but MRB did not receive any follow-up from MassIT about when and how the DR test would be conducted and did not follow up with MassIT itself for fiscal year 2015 or 2016.

c. MRB did not have backup policies and procedures for its internal FTP server.

MRB did not have policies and procedures to manage backup activity for its internal FTP server. Furthermore, MRB could not provide evidence that a full backup had been performed during the audit period. Partial backups had been performed and kept at the same physical location as the server, but there were no offsite backups of any kind. This increases the risk of MRB permanently losing protected information in the event of a business interruption or disaster.

Authoritative Guidance

MassIT's Enterprise Communications and Operations Management Policy states,

> *Agencies are required to develop and implement backup procedures to ensure that backup of systems and data and verification testing are performed, schedules and backup documentation are written, and storage locations chosen, in accordance with industry best practices and agency security requirements.*

The National Institute of Standards and Technology (NIST) Special Publication 800-34 states,

> *System data should be backed up regularly. Policies should specify the minimum frequency and scope of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. Data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. . . .*
>
> ***It is good business practice to store backed-up data offsite****.* [Emphasis added.]

Reasons for Noncompliance

MRB management told us that they did not have policies and procedures for backups and that they followed MassDOT IT's ISP. We found that the ISP had no specific section regarding backups. Therefore, we concluded that MRB management was not aware of their responsibility of documenting, developing, and implementing backup procedures. They also did not designate an employee responsible for the development of backup policies and procedures.

Recommendations

1. MRB should work with MassDOT IT to develop, document, and implement a BCP that includes MRB operations.

2. MRB should consult with MassDOT to perform a DR test for all critical information technology (IT) assets (such as data, equipment, IT services, and IT personnel) to ensure that suitable alternative procedures exist in case disruptions occur. The DR test should be performed annually to minimize the duration of any disruption to MRB operations.

3. MRB should consult with MassDOT to document, develop, and implement backup procedures for its servers. These procedures should ensure that full offsite backups are performed and maintained regularly.

Auditee's Response

The Merit Rating Board has no control of infrastructure on which to conduct DR testing and all ALARS data is shared between the Merit Rating Board and the Registry of Motor Vehicles. It would not be possible for the Merit Rating Board to create a BUSINESS Continuity Plan (BCP) or conduct any Disaster Recovery testing independent of MASSDOT IT and MASS IT.

The Merit Rating Board has provided documentation to MASSDOT IT & MASSIT whenever requested concerning the Merit Rating Board requirements for business continuity and disaster recovery. The creation of a formal BCP and all disaster testing must be done as part of an overall effort on the part of MASSDOT IT with the Merit Rating Board as one of the subdivisions within that effort. . . .

The Merit Rating Board no longer has control over the data servers and workstation infrastructure within our department. We are dependent on MASSDOT IT to provide backup and recovery for this data. It is our understanding that the data servers are backed up regularly and a set of backups is routinely sent to an offsite location. These Recommendations will be directed appropriately to MASSDOT IT.

Auditor's Reply

We acknowledge that MRB does not have control over infrastructure and ALARS data. This is why we recommend that MRB consult with MassDOT in developing a BCP and performing a DR test for all critical IT assets (such as data, equipment, IT services, and IT personnel) to ensure that suitable alternative procedures exist in case disruptions occur. MRB needs to work with MassDOT IT to develop, implement, test, and maintain a BCP for all IT resources that deliver and support core critical business functions of MRB.

Further, we acknowledge that MRB was in the process of moving its data servers and workstations under MassDOT IT operations during our audit period. However, the Office of the State Auditor believes MRB should still take measures to ensure that its data servers are backed up regularly by MassDOT IT and maintained off site.