



**STATE OF MISSISSIPPI  
OFFICE OF THE STATE AUDITOR  
STACEY E. PICKERING  
STATE AUDITOR**

**December 18, 2014**

**Information Systems Management Report**

J. Ed Morgan, Commissioner of Revenue  
Mississippi Department of Revenue  
500 Clinton Center Drive  
Clinton, Mississippi 39056

Dear Commissioner Morgan:

The Office of the State Auditor has completed its limited assessment of the Information Systems (IS) general controls and selected application controls of the Mississippi Department of Revenue (MDOR). This assessment focused on the adequacy of the MDOR information technology general controls (ITGC) which help to protect the integrity and security of its computer systems and was performed in conjunction with the audit of the State of Mississippi.

The following members of the Office of the State Auditor participated in this engagement: David Ashley, MBA, ME, CISA, CISM, CBCP, CRISC (IS Audit Director), Mike Ferguson, CISA (IS Audit Manager) and LaDonna Johnson, MBA, CISA (Senior IS Auditor).

Scope of Our Review

To support our general controls assessment, our procedures were performed through observations, discussions and testing of the information technology general controls (ITGC) of the Mississippi Department of Revenue's Information Systems. The scope of our Information Systems review included information processing technology risks in the following categories: integrity, reliability, availability and access, managing problems and incidents.

Limitations

In planning and performing our limited assessment of Mississippi Department of Revenue's Information Systems, we considered Mississippi Department of Revenue's information technology general controls (ITGC) in order to determine our assessment procedures; however, this review was not for the purpose of expressing an opinion on the effectiveness of the internal control over information systems. Also, these procedures cannot and do not provide absolute assurance that all state legal requirements have been met. In accordance with Section 7-7-211, Miss. Code Ann. (1972), the Office of the State Auditor, when deemed necessary, may conduct additional procedures for this or other fiscal years to ensure compliance with legal requirements.

## Internal Controls Over Information Systems

As stated previously, our review was intended to be in support of the state financial audit of the Mississippi Department of Revenue. Therefore, any exceptions in ITGC are ultimately evaluated as to their impact on financial reporting by the entity.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis. A material weakness is a deficiency or combination of deficiencies in internal control such that there is a reasonable possibility, that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency or a combination of deficiencies in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.

Our consideration of the internal controls over IS was for the limited purpose described in the fourth paragraph and was not designed to identify all deficiencies in internal control over information systems that might be material weaknesses or significant deficiencies and therefore material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our review we did not identify any deficiencies in internal control that we consider to be material weaknesses.

## Compliance

As part of obtaining reasonable assurance about whether selected IS general controls of the Mississippi Department of Revenue are functioning as designed, we performed assessments of compliance with industry best practices. However, providing an opinion on compliance with these practices was not an objective of our assessment and accordingly, we do not express such an opinion.

## Summary

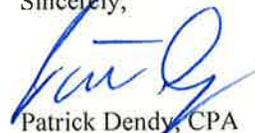
We identified a deficiency involving internal control over ITGC that we consider to be a significant deficiency in internal control over IS. This matter is noted under the heading SIGNIFICANT DEFICIENCY. We also noted deficiencies in internal control over ITGC that we consider to be control deficiencies which are under the heading CONTROL DEFICIENCIES. Please review the recommendations included in this report and submit a plan to implement them by January 16, 2015. The enclosed findings contain more information about our recommendations. During future engagements, we may review the findings in this engagement report to ensure that procedures have been initiated to address this report.

## Purpose of this Report

The purpose of this report is solely to describe the scope of our general controls assessment of the Mississippi Department of Revenue's Information Systems and the results of that assessment. Accordingly, this communication is not suitable for any other purpose. However, this report is a matter of public record and its distribution is not limited.

We appreciate the cooperation and courtesy extended by the officials and employees of the Mississippi Department of Revenue throughout this review. If you have any questions or need more information, please contact me.

Sincerely,



Patrick Dendy, CPA  
Director, Department of Audit

Enclosures

**OFFICE OF THE STATE AUDITOR  
 INFORMATION SYSTEMS MANAGEMENT REPORT  
 MISSISSIPPI DEPARTMENT OF REVENUE  
 AS OF SEPTEMBER 24, 2014**

**TABLE OF CONTENTS**

	Page No.
I. ABBREVIATIONS USED IN THIS REPORT .....	4
II. REVIEW OBJECTIVES AND APPROACH .....	4
III. STANDARDS FOR BEST PRACTICES .....	5
IV. FINDINGS AND RECOMMENDATIONS .....	5
<u>SIGNIFICANT DEFICIENCY</u>	
Finding 1. MDOR Should Become Compliant with Federal Mandates .....	5
<u>CONTROL DEFICIENCIES</u>	
Finding 2. Formal Policies and Procedures Do Not Adequately Cover All Areas of Information Technology. ....	6
Finding 3. DOR Should Conduct Periodic Formal Access Reviews (Physical and Logical).....	7
Finding 4. MDOR Should Implement a Formal Information Security Policy .....	7
Finding 5. MDOR Should Provide for Regular Network Security Reviews .....	8
Finding 6. Backup Power for IT Equipment at ABC Should Be Established .....	8
Finding 7. ABC Should Update Its Disaster Recovery Plan and Test the Updated Plan.....	9

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF REVENUE  
AS OF SEPTEMBER 24, 2014**

I. ABBREVIATIONS USED IN THIS REPORT

ABC	Alcohol Beverage Control
ACT	Federal Anti-Theft Act of 1992
FAST	FAST Enterprises, LLC
FISCAM	Federal Information Systems Controls Audit Manual
IS	Information Systems
IT	Information Technology
ITGC	Information Technology General Controls
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
ITS	Mississippi Department of Information Technology Services
MIS	Management Information Systems
OSA	Office of the State Auditor
MARS	Mississippi Automated Revenue System
MDOR	Mississippi Department of Revenue
PII	Personally Identifiable Information

II. REVIEW OBJECTIVES AND APPROACH

Our review's overall objective was to perform an assessment of the general data processing controls established by management of the Mississippi Department of Revenue to support the integrity and security of the information processed by the computer systems of the Mississippi Department of Revenue at its main office in Clinton, Mississippi. To accomplish these objectives, the Information Systems Audit Section staff of the Office of the State Auditor (OSA):

- Met with Mississippi Department of Revenue management and the OSA auditors to gain an understanding of the critical Mississippi Department of Revenue processes and controls;
- Interviewed selected Mississippi Department of Revenue technology and accounting personnel;
- Reviewed available documentation of procedures, standards and other evidential matter;
- Identified any vulnerabilities associated with any weaknesses, if noted, in the control environment.

Our approach was not designed to specifically detect illegalities, fraudulent acts, errors or other irregularities.

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF REVENUE  
AS OF SEPTEMBER 24, 2014**

III. STANDARDS FOR BEST PRACTICES

In this report we will refer to best practices standards that should be achieved by all Information Technology (IT) departments. Specifically we mention and utilize the methodology of CobiT 4.0 of the IT Governance Institute ([www.itgi.org](http://www.itgi.org)) as the industry standard we have selected for the evaluation of the IT control environment. Other similar methodology is the Information Technology Infrastructure Library (ITIL) which is a framework of best practice approaches intended to facilitate the delivery of high quality IT services. ITIL outlines an extensive set of management procedures that are intended to support businesses in achieving both quality and value for money in IT operations. These procedures are supplier independent and have been developed to provide guidance across the breadth of IT infrastructure, development, and operations.

Additional sources for Information Systems control criteria include *The State of Mississippi Department of Information Technology Services' Enterprise Security Policy* and the U. S. Government Accountability Office's Federal Information System Controls Audit Manual (FISCAM). This manual provides guidance for reviewing information system controls affecting integrity, confidentiality, and availability of computerized data. See <http://www.gao.gov/products/GAO-09-232G>.

IV. FINDINGS AND RECOMMENDATIONS

SIGNIFICANT DEFICENCY

1. MDOR Should Become Compliant with Federal Mandates.

*Finding:*

The Title and Motor Vehicle system currently being used by MDOR is out of compliance with federal mandates concerning the Federal Anti-Car Theft Act of 1992 (ACT). This act calls for states to be able to provide information about vehicle ownership on a real time basis. The existing system cannot meet this mandate nor can it be enhanced or improved. Also outages of the system have occurred in the past and the system is subject to failure at any time. A failure in the system means the public is unable to buy or sell automobiles until the system can be recovered and subsequently titles can be issued. It is estimated that ad valorem revenue would be delayed at a cost of \$1.1 million per day if the system were to fail.

*Recommendation:*

MDOR should move to replace this critical system as soon as possible in order to avoid loss of services to the public and the delay of income to the counties, municipalities and local school boards. Additionally the State of Mississippi could face sanctions and possible fines from the federal government, due to failure to comply with regulations such as the Federal Anti-Car Theft Act of 1992 (ACT). Mississippi is one of only three states that do not comply with this law.

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF REVENUE  
AS OF SEPTEMBER 24, 2014**

CONTROL DEFICIENCIES

2. Formal Policies and Procedures Do Not Adequately Cover All Areas of Information Technology.

*Finding:*

CobIT PO6.3 calls for organizations to “Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.”

The ITS Enterprise Security Policy Part I, Chapter 1, Rule 1.11F states “Each Agency must develop, implement, and maintain their individual agency IT security policy. Each agency will annually review and revise (as needed) its security policy.”

Mississippi Department of Revenue (MDOR) has policies and procedures that relate specifically to Information Technology (IT) as well as policies and procedures that are applicable at an agency level yet are IT in nature. Examples of policies and procedures that are IT specific include Backup Retention Policy, Information Security Plan and Password Policy while agency policies that are IT in nature include Use of Communication and Computing Policies and Procedures as well as Personal Use of Social Media Policy.

While the IT related policies and procedures that do exist for MDOR are well prepared and understandable, there are areas not covered in these policies and procedures that should be of great concern to an organization the size, complexity and importance of MDOR. These areas include Data Breach Management, Encryption, and Change Management.

Not having formal policies that cover all areas that are pertinent to an organization causes confusion to employees as well as management in making business decisions. Without supporting policies, actions become difficult to defend in situations such as employee discipline and regulatory compliance. In addition policies and procedures involving the handling of breeches and disaster recovery can greatly facilitate the recovery of data and restrict further damage in critical situations.

*Recommendation:*

While ITS policies can certainly be used as a guideline for agency policies and procedures, each agency must have its individual policies and procedures as stated above. Policies should be general enough in nature to serve as guidelines for the area to be covered yet specific enough to cover the areas of governance for the agency where guidance might be needed. Also, these polices should be reviewed and changed accordingly on at least an annual basis or more frequently if business process changes dictate a need to do so. Management should approve all policies and procedures, as well as changes to these documents. In addition a system that is appropriate to organizational culture should be developed to disseminate policies and procedures and any related changes to applicable parties in a timely manner. Documentation of such changes, approved by management and accepted by employees, should be retained for later review by auditors.

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF REVENUE  
AS OF SEPTEMBER 24, 2014**

3. DOR Should Conduct Periodic Formal Access Reviews (Physical or Logical).

*Finding:*

Although MDOR does have formalized procedures for gaining and terminating access to data assets, our audit indicated that formalized access reviews are not consistently conducted at MDOR. In addition, policies do not specifically cover the performance of such reviews.

CobiT PO7.8 states that organizations should, "Take expedient actions regarding job changes, especially job terminations. Knowledge transfer should be arranged, responsibilities reassigned and access rights removed such that risks are minimized and continuity of the function is guaranteed."

Not performing access reviews considerably increases the risk of unauthorized access of information assets and therefore increases the probability of a data breach that could significantly affect the daily operations of MDOR and the Personally Identifiable Information (PII) of the taxpayers of the state of Mississippi.

*Recommendation:*

It is recommended that policies be modified to provide that access reviews be performed on at least an annual basis for logical access to data assets as well as physical access to areas where hardware used to access these data assets resides. Reviews for both physical and logical access to all information assets should be conducted at least annually or more frequently according to changes that dictate such a review. Evidence of such reviews should be signed, dated and retained for appropriate periods for later audit review.

This access review should specifically include review of access to the computer room at MDOR headquarters in Clinton. Considering that the MARS implementation is ongoing and that many of the legacy systems will be "sunset" in the near future, it is recommended that access to the computer room be reviewed on a periodic basis such as every six (6) months in order to provide adequate protection to data resources during this very vulnerable period.

4. MDOR Should Implement a Formal Information Security Policy.

*Finding:*

During our review of information system controls at the Department of Revenue we noted the agency has not adopted a formal Information Security Policy or Enterprise Security Plan.

During 2009, the *State of Mississippi Department of Information Technology Services' Mississippi ITS Enterprise Security Policy* was substantially updated and strengthened and requires all state agencies to have a written information security plan, conduct a security risk analysis, implement a data classification scheme, and provide for periodic external security reviews.

The lack of a formal Information Security Policy can lead to a breakdown of basic security practices in the area of application security, LAN/WAN security, management of the security application, and Internet protocol.

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF REVENUE  
AS OF SEPTEMBER 24, 2014**

*Recommendation:*

Practices outlined in the *State of Mississippi Department of Information Technology Services' Mississippi ITS Enterprise Security Policy* are typical of appropriate standards for any moderate sized IT organization. While full compliance with all facets of the policy may be an economic challenge for MDOR, beginning steps to become compliant with the policy are necessary. We recommend that MDOR create a plan of compliance with industry standards and State policy to ensure progress towards a more robust documented information security plan.

5. MDOR Should Provide for Regular Network Security Reviews.

*Finding:*

The *State of Mississippi Department of Information Technology Services' Enterprise Security Policy* requires that internal system and network security audits be performed every three years by a third party or whenever a major change has occurred within the agency. MDOR has had a change in that they have moved their computer center to a new site and in accordance with the *State of Mississippi Department of Information Technology Services' Enterprise Security Policy* they should have a third party come in and perform a security review.

*Recommendation:*

MDOR should implement a plan to insure it complies with *the State of Mississippi Department of Information Technology Services' Enterprise Security Policy* and its own security policy as soon as possible.

6. Backup Power for IT Equipment at ABC Should Be Established

*Finding:*

As a result of our audit, we concluded that there are no backup electrical generators at ABC that would provide power to maintain access to IT related systems in the event of a power failure. CobiT DS4.3 addresses the need for continuous uninterruptable power systems (UPS) be maintained which would allow computer equipment to be brought down in a controlled manner in case of an extended power failure. Failure to assure power to computer equipment in a controlled manner during a power outage could cause loss of user access, loss of revenue, loss of data and equipment damage.

*Recommendation:*

We recommend that key equipment be attached to a backup power generation source that is maintained and tested in line with best business practices to ensure continued service in the event of a power failure or other interruption. The risk involved in not having such equipment in place is increased due to the significant effort being given to convert business processes to a "paperless" environment.

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF REVENUE  
AS OF SEPTEMBER 24, 2014**

7. ABC Should Update Its Disaster Recovery Plan and Test The Updated Plan.

*Finding:*

In the course of our audit we were told that although ABC has a disaster recovery plan, it has not been recently updated and that it is not being tested on a periodic basis. Disaster recovery involves defining and documenting plans to help sustain and recover critical information technology resources, information systems, and associated business functions. *Control Objectives for Information and Related Technology* (CobiT, Section DS4), as well as recognized industry best practices, require a written disaster recovery plan be developed and tested regularly to provide orderly recovery of vital functions in the event of a hardware or environmental disaster. Failure to test recovery plans and systems could result in the non-discovery of system incompatibilities, capacity planning issues, and other information technology driven significant issues. Although implementation of the portion of MARS that will replace the present ABC financial systems is scheduled to occur in 2015, it is imperative that present financial systems be determined recoverable. A new AS/400 was recently installed at ABC, which runs the financial software at ABC, therefore increasing the risk for outages.

*Recommendation:*

We recommend that the Alcoholic Beverage Control update as well as implement a disaster recovery test or walkthrough for the IT Disaster Recovery Plan documenting the results as well as any problems occurring during the process. The installation of the new AS/400, which runs the financial software at ABC, makes the updating and testing of the disaster recovery plan very important.

**End of Report**