



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

February 2, 2010

**Information Systems Management Report**

J. Ed Morgan  
Chairman and Commissioner of Revenue  
Mississippi State Tax Commission  
1577 Springridge Road  
Raymond, Mississippi 39154

Dear Mr. 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 Office of Information Technology of the Mississippi State Tax Commission (MSTC). This assessment focused on the adequacy of MSTC's 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: Toby Frazier, CISA (IS Audit Section Director), Mike Ferguson, CISA (Senior IS Auditor), LaDonna Johnson, MBA (Senior IS Auditor) and Jason Johnston, MPA (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 MSTC's Information Systems. Our fieldwork for these assessment procedures was begun on July 7, 2009. 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. We also performed selected tests on application system data as requested by the OSA Agency Audit Section, and conducted a preliminary review of the "Titanium" collections application system to be implemented at MSTC.

Limitations

In planning and performing our limited assessment of MSTC's information systems, we considered MSTC'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.

## Standards for Reporting of Findings

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

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

Our consideration of the internal control over IS was for the limited purpose described in the fourth paragraph and would not necessarily identify all deficiencies in internal control over information systems that might be significant deficiencies or material weaknesses.

## Summary

We did not identify any deficiencies in the general controls that we consider to be a material weakness, as defined above. However, we noted certain other deficiencies in general controls that require the attention of management. These matters are noted under the heading SIGNIFICANT DEFICIENCIES IN INTERNAL CONTROL. As part of obtaining reasonable assurance about whether selected IS general controls of the Mississippi State Tax Commission were functioning as designed, we performed assessments of compliance with industry best practices. However, providing an opinion on compliance with those practices was not an objective of our assessment and, accordingly, we do not express such an opinion.

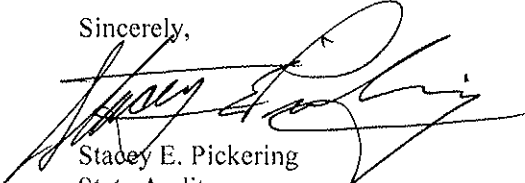
Please review the recommendations included in this report and submit a plan to implement them by, February 24, 2010. The enclosed findings contain more information about our recommendations.

During future engagements, we may review the findings in this management report to ensure procedures have been initiated to address these findings.

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

This report is intended solely for the information and use of management, Members of the Legislature and federal awarding agencies and is not intended to be and should not be used by anyone other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

Sincerely,



Stacey E. Pickering  
State Auditor

Enclosures

OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI STATE TAX COMMISSION  
AS OF JULY 31, 2009

**TABLE OF CONTENTS**

|  | Page No. |
|--|----------|
| I. ABBREVIATIONS USED IN THIS REPORT .....                             | 2        |
| II. REVIEW OBJECTIVES AND APPROACH .....                               | 3        |
| III. STANDARD OF BEST PRACTICES .....                                  | 3        |
| IV. FINDINGS AND RECOMMENDATIONS .....                                 | 4        |
| <br><u>SIGNIFICANT DEFICIENCIES IN INTERNAL CONTROL</u>                |          |
| Finding 1. MSTC Should Implement a Formal IT Management Framework..... | 4        |
| Finding 2. MSTC Should Document an Information Security Plan.....      | 5        |
| Finding 3. MSTC Should Create a Disaster Recovery Plan for ABC.....    | 6        |
| <br><u>CONTROL DEFICIENCIES</u>  |          |
| Finding 4. MSTC Should Improve Its Physical IT Environment.....        | 7        |

OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI STATE TAX COMMISSION  
AS OF JULY 31, 2009

I. ABBREVIATIONS USED IN THIS REPORT

|        |                                       |
|--------|---------------------------------------|
| ABC    | Office of Alcoholic Beverage Control  |
| IS     | Information Systems                   |
| IT     | Information Technology                |
| LAN    | Local Area Network                    |
| MSTC   | Mississippi State Tax Commission      |
| Novell | LAN operating system from Novell Inc. |
| OIT    | Office of Information Technology      |
| OSA    | Office of the State Auditor           |

OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI STATE TAX COMMISSION  
AS OF JULY 31, 2009

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 State Tax Commission (MSTC) that support the integrity and security of the financial information processed by the computer systems of the MSTC at its main office in Raymond, Mississippi, and the Office of Alcoholic Beverage Control's (ABC) general offices in Madison, Mississippi.

To accomplish these objectives, the Information Systems Audit Section staff of the Office of the State Auditor (OSA):

- Met with MSTC management and the OSA financial auditors to gain an understanding of the critical MSTC processes, and controls;
- Interviewed key MSTC OIT personnel, and selected MSTC and ABC management;
- Reviewed available documentation of procedures, standards and other evidential matter;
- Performed audit tests to verify the existence and effectiveness of the controls, and processes in place to meet the objectives delineated above; and
- 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.

III. STANDARD OF 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 recommend the methodology of COBIT 4.1 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. The need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are key elements of enterprise governance. Value, risk and control constitute the core of IT governance.

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.

NIST.gov from the National Institute of Standards and Technology, Information Technology Laboratory also provides guidance on best practices for computer security, including Federal Information Processing Standards, (FIPS).

IV. FINDINGS AND RECOMMENDATIONS

**SIGNIFICANT DEFICIENCIES IN INTERNAL CONTROL**

**1. MSTC Should Implement a Formal IT Management Framework**

*Finding:*

**New Titanium Application and Its Security Was Not Documented**

Like many organizations that use legacy systems, MSTC has very limited to no documentation for its core application systems; therefore, most standards and procedures are informal. There is also limited documentation and written policies and procedures for client/server and network systems.

Skilled information technology specialists, many of whom have over 20 years of experience staff the OIT (Office of Information Technology) at MSTC. Many day-to-day practices are generally comparable to those found in organizations of similar size and complexity, however, informal controls based on years of experience and personal interaction are much more predominate than written policies and procedures.

In our 2006 Information Systems Management Report we published a finding which stated MSTC should document its key systems and processes, develop and maintain standards and procedures for the data processing function. Documented planning and processes are key to effective IT control. MSTC has an informal structure in place but it varies totally from system to system, and IT manager to manager, as to what is considered necessary for standards and procedures, and none is documented.

In 2008 we noted in our audit report a lack of key internal control activities of program version control in the key Legacy Sales application, which seems to trace to the year 2000 conversion process. Issues such as this may result due to the absence of strict formal written standards.

In 2009, MSTC added a new commercial application system known as "Titanium" to manage its collections activities. During our review of the implementation process of Titanium, other than vendor supplied documentation, we were unable to locate any planning documents, including any standards and procedures for the interfaces to this system, or documentation or processes as to how the application was to reconcile with the primary MSTC application systems balances. Also, no information security plan was located for this system. User privileges had been set up through the MSTC Novell LAN, but the security functions and roles were undocumented, and the lack of a formal documented security scheme prevented an effective audit of the application security.

MSTC appears to be on the threshold of a new integrated application system to replace the multiple unrelated systems which have been layered in over the years. While this application may hold the promise of improved performance and tax compliance, unless a consistent and documented methodology of system standards and procedures is implemented, quality and consistency of security, and control requirements may not be implemented, understood, or result

OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI STATE TAX COMMISSION  
AS OF JULY 31, 2009

as insufficient. The investment in the application could also deteriorate over the ensuing years as changes may not be documented and controls also could become lax.

*Recommendation:*

We recommend that MSTC OIT begin to implement a framework that would provide for more consistent standards and procedures throughout the OIT division. A formal framework of IT Governance should be established that would include many activities that will not change with the implementation of new application software, such as LAN practices and standards, network standards and information security (see next finding). Once new application software is implemented MSTC should maintain standards to keep this application's documentation and standards current to help prevent degradation of control, reliability and security of the application.

Currently, MSTC should appropriately document the Titanium application and the security practices associated with this application to correspond with an IT Governance plan.

**2. MSTC Should Document an Information Security Plan**

*Recurring Finding:*

**MSTC Had No Formal Information Security Policy**

Since our 2006 Information Systems Management Report we have communicated the need for MSTC to implement a formal Information Security Policy or Enterprise Security Plan. This finding also relates to our first finding in this report, as a strong security stance is a function of a strong IT Governance process.

To our 2006 IS Management Letter, management of MSTC responded affirmatively that they would comply to this requirement of the *Mississippi State Enterprise Security Policy*. Again, this was listed as an exception in our 2007 report with a completion date expected in 2008. During this review we inquired to obtain a copy of the Information Security Plan, but no written plan was available.

During 2009, the *Mississippi State Enterprise Security Policy* has been substantially updated and strengthened and requires all state agencies to have a written information security plan, conduct security risk analysis, implement a data classification scheme, and provide for periodic external security reviews.

*Recommendation:*

Practices outlined in the *Mississippi State 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 MSTC, beginning steps to become compliant with the policy are necessary. We recommend that MSTC create a plan of compliance with industry standards and State policy to provide concrete progress towards a more robust documented information security plan.

OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI STATE TAX COMMISSION  
AS OF JULY 31, 2009

**3. MSTC Should Create a Disaster Recovery Plan for ABC**

*Recurring Finding:*

**ABC Had No Disaster Recovery Plan**

During our review procedures, we noted ABC did not have a formal written disaster recovery plan. Without a tested written disaster contingency plan in place, recovery efforts at ABC could be significantly delayed or even harmed in the event of a disruption, resulting in impaired revenue to the State of Mississippi. This has been noted in our reports since at least 2006.

Systems availability is a key control issue for any organization; this is supported by CobiT DS4 Deliver and Support, which sets standards for the development of an IT Continuity Framework, DS4.1 and continuing on through DS4.10 with standards which describe the entire contingency planning process.

*Recommendation:*

We recommend that the MSTC Information Technologies disaster recovery plan include services at ABC. Such plans for ABC should coordinate with MSTC Information Technologies plans, and should be reviewed and tested at least on an annual basis.

## CONTROL DEFICIENCIES

### 4. MSTC Should Improve Its Physical IT Environment

*Recurring Finding:*

**The MSTC Physical Environment for Its Computers and Security is Sub-standard**

Tax related systems contain some of the most critical individual personal identification data held by the State. Reliability of these systems is also paramount to the State's ability to collect a steady stream of revenue. However, the physical environmental attributes for these critical computer applications is among the worse of any state agency. MSTC's critical systems are housed in built-out rooms within the leased metal building of MSTC headquarters. Although entry to the rooms is controlled by zoned access cards, the physical protection of the equipment is poor. Roof leaks over the computer rooms are evident by water stained ceiling tiles and discarded water damaged tiles. Fire suppression systems contain live water pipes above the computer equipment. Computer equipment rooms should not be protected by water based fire suppression sprinkler systems, especially those with "wet-pipe" applications. The emergency power cut-off switch in the computer room is located in an inappropriate place and has been supplemented by a cardboard cover to help prevent misuse. The building does not have back-up generator power, as do the other large state agencies with computer systems. The computer rooms are not hardened for sufficient protection from severe weather incidents.

At ABC there is no card access system to protect the computer room or the office space, but instead an honor system log is maintained for access to the computer room. Times exist where no staff is present in the computer room, and although a policy exists for the door to be manually locked, this is not always possible to enforce.

*Recommendation:*

MSTC should take the physical shortcomings of its facilities into account as part of an overall security risk analysis process. The risk of water damage to key server equipment appears to be the most prevalent but an analysis should point out actions to be taken to mitigate such risks.

**End of Report**