



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

June 30, 2010

Information Systems Management Report

Honorable J. Tate Reeves, State Treasurer
State Treasury Department
P. O. Box 138
Jackson, Mississippi 39205

Dear Mr. Reeves,

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 State Treasury Department. This assessment focused on the adequacy of Treasury'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: 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 Treasury's Information Systems. Our fieldwork for these assessment procedures was begun on May 3, 2010. 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 Treasury's information systems, we considered Treasury'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 Mississippi State Treasury Department. 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 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 financial statements will not be prevented or detected. A significant deficiency is a deficiency or 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 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 and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have been identified.

Summary

Our review of ITGC of Treasury's Information Systems Division did not identify any deficiencies in the internal control over IS and its operation that we consider to be a material weakness, as defined above. However, we noted certain deficiencies involving internal control over ITGC that require the attention of management. These matters are noted under the heading CONTROL DEFICIENCIES. As part of obtaining reasonable assurance about whether selected IS general controls of the Mississippi State Treasury Department were functioning as designed, we performed assessments of compliance with certain regulations and 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.

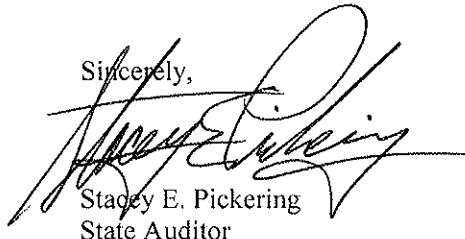
Please review the recommendations included in this report and submit a plan to implement them by, July 16, 2010. The enclosed findings contain more information about our recommendations.

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 Treasury Department 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 TREASURY DEPARTMENT
AS OF JUNE 30, 2010**

TABLE OF CONTENTS

	Page No.
I. ABBREVIATIONS USED IN THIS REPORT	4
II. REVIEW OBJECTIVES AND APPROACH	5
III. STANDARDS FOR BEST PRACTICES	5
IV. FINDINGS AND RECOMMENDATIONS	6
 <u>CONTROL DEFICIENCIES</u>	
Finding 1. State Treasury Department Should Comply with Requirements of its Security Policy Concerning Passwords	6
Finding 2. State Treasury Department Should Consider Other Options for Fire Suppression in the Computer Room	6

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI TREASURY DEPARTMENT
AS OF JUNE 30, 2010**

I. ABBREVIATIONS USED IN THIS REPORT

QED	QED Financial Systems
LAN	Local Area Network
IS	Information Systems
IT	Information Technology
ITS	Mississippi Department of Information Technology Services
OSA	Office of the State Auditor

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI TREASURY DEPARTMENT
AS OF JUNE 30, 2010**

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 Treasury Department to support the integrity and security of the information processed by the computer their systems. To accomplish these objectives, the Information Systems Audit Section staff of the Office of the State Auditor (OSA):

- Met with Treasury management and the OSA financial auditors to gain an understanding of the critical Treasury processes and controls;
- Interviewed selected Treasury technology and accounting personnel;
- Reviewed available documentation of procedures, standards and other evidential matter;
- Performed audit tests to verify the existence and effectiveness of the processes and controls 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. 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) 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. General Accounting 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>.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI TREASURY DEPARTMENT
AS OF JUNE 30, 2010**

IV. FINDINGS AND RECOMMENDATIONS

A. CONTROL DEFICIENCIES

Finding:

1. State Treasury Department Should Comply with its Security Policy Concerning Passwords.

The security department sets all the passwords for the users in the Treasury Department. This is a direct violation of its security policy which states, "4.1 passwords must not be disclosed to anyone except in emergency circumstances or when there is an overriding operational necessity". Also the user ids and passwords are written down and kept in the IT director's desk which is another violation of policy, 4.3 states, " Passwords must never be written down". A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource (example: an access code is a type of password). The practice of someone other than the user knowing the password renders the password useless for authentication purposes.

Recommendation:

We recommend that the State Treasury Department cease the practice of resetting user's passwords and documenting the individual user's passwords. The user should be allowed to set his/her own password to a string of characters known only by the user and no one other than the user.

2. State Treasury Department Should Consider Other Options for Fire Suppression in the Computer Room.

Finding:

The State Treasury Department utilizes a fire suppression system called "wet pipe". This means there is water in the overhead pipes at all times. Any damage to these pipes could cause the water to disperse or leak onto the computer equipment possibly causing a disruption of service.

Recommendation:

The State Treasury Department should explore the feasibility of acquiring a more current fire suppression system which does not utilize the "wet pipe" solution and minimize the risk of water damaging their computer equipment.

End of Report