



**STATE OF MISSISSIPPI**  
**OFFICE OF THE STATE AUDITOR**  
**PHIL BRYANT**  
AUDITOR

December 19, 2006

**Information Systems Management Report**

Honorable J. Tate Reeves, State Treasurer  
State of Mississippi  
501 N. West St.  
1101-A Woolfolk Building  
Jackson, Mississippi 39201

Dear Mr. Reeves:

The Office of the State Auditor has completed its limited assessment of the EDP general controls of the State Treasury Department for the year ended June 30, 2006. This assessment was performed in conjunction with the audit of the financial statements of the State of Mississippi. The Office of the State Auditor's staff member participating in this EDP review engagement was Toby Frazier, CISA.

The fieldwork for these assessment procedures was completed on August 24, 2006. 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.

In planning and performing our limited assessment of the EDP general controls, we considered the State Treasury Department's internal control over electronic data processing in order to determine our assessment procedures and not to provide an opinion on the internal control over electronic data processing. These procedures were performed primarily through observations and discussions with State Treasury Department personnel.

Our consideration of the internal control over electronic data processing would not necessarily disclose all matters in the internal control that might be a material weakness. A material weakness is a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. We noted no matters involving the internal control over electronic data processing and its operation that, we consider to be a material weakness.

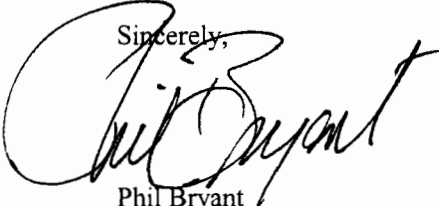
However, we noted certain immaterial weaknesses involving internal control over electronic data processing that require the attention of management. These matters are noted under the heading IMMATERIAL WEAKNESSES IN INTERNAL CONTROL. As part of obtaining reasonable assurance about whether selected EDP general controls of the State Treasury Department were functioning as designed, we performed assessments of compliance with certain regulations and industry best practices. Providing an opinion on compliance with those regulations and 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 January 12, 2007. 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.

This report is intended solely for the information and use of management and Members of the Legislature 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.

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

Sincerely,  
  
Phil Bryant  
State Auditor

Enclosures

**OFFICE OF THE STATE AUDITOR  
EDP GENERAL CONTROLS ASSESSMENT  
OF THE STATE OF MISSISSIPPI  
TREASURY DEPARTMENT  
AS OF FYE JUNE 30, 2006**

**TABLE OF CONTENTS**

	Page No.
I. REVIEW OBJECTIVES AND APPROACH .....	4
II. STANDARD OF BEST PRACTICES .....	4
III. FINDINGS AND RECOMMENDATIONS	
<u>IMMATERIAL WEAKNESSES IN INTERNAL CONTROL</u>	
1. QTMS Passwords Should be Rotated on a Regular Basis.....	5
2. QTMS User Rights Should Be Reviewed.....	5
3. Internal Network Should be Bannered.....	6
4. Physical Access To Critical Servers Should Be Limited.....	6

OFFICE OF THE STATE AUDITOR  
EDP GENERAL CONTROLS ASSESSMENT  
OF THE STATE OF MISSISSIPPI  
TREASURY DEPARTMENT  
AS OF FYE JUNE 30, 2006

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 State Treasury Department which supports the integrity and security of the state's financial information. To accomplish these objectives, the EDP Audit Section staff of the Office of the State Auditor (OSA):

- Met with State Treasury Department management and the OSA financial auditors to gain an understanding of the critical State Treasury Department EDP systems, processes, and controls;
- Interviewed key State Treasury Department technology personnel;
- Reviewed available documentation of procedures, standards and other evidential matter;
- Performed tests to verify the existence and effectiveness of the EDP 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.

STANDARD OF BEST PRACTICES

In this report we will refer to best practice standards that should be achieved by all Information Technology (IT) departments. Specifically, we mention and endorse the methodology of *Control Objectives for Information and Related Technology* (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.

OFFICE OF THE STATE AUDITOR  
EDP GENERAL CONTROLS ASSESSMENT  
OF THE STATE OF MISSISSIPPI  
TREASURY DEPARTMENT  
AS OF FYE JUNE 30, 2006

Instances of Immaterial System Weaknesses/Deficiencies Identified During the Review

We have identified certain weaknesses / deficiencies during our review of the computer processing controls which we feel are immaterial in nature but believe management should be made aware of. These weaknesses are presented along with our recommendation for improving those weaknesses.

1. Treasury's QED Financial Systems OTMS Passwords Should Be Rotated on a Regular Basis

*Finding:*

Our review of the user definitions within the QED Financial Systems' Treasury Management System (QTMS) application indicated that user passwords were set to never expire. This indicates that QTMS passwords may never have been rotated for some period of time.

The application user links to QTMS through its Windows account (which did have password rotation in effect), but we determined that this was not a hard link, and the two accounts were not connected for security verification. Therefore, it could be possible for a user to use another's QTMS user-id and password, if known. Lack of application password rotation amplifies this exposure.

This principle is supported by CobiT DS5 *Ensure Systems Integrity, DS 5.3 Identity Management* which suggests that all users and their activity on IT systems should be uniquely identifiable.

*Recommendation:*

We recommend that the QED Treasury Management System (TMS) user passwords be rotated on regular defined basis.

2. Treasury's QED Financial Systems TMS User Rights Should Be Reviewed

Within the QTMS application are tables of function rights which have been granted to system users. We noted nine individuals and a generic administration ID were granted authority to modify, delete or add items to the warrant reconciliation files. Some of these rights granted appear to be in conflict with separation of duties, which could lead to inappropriate or unauthorized modifications to the warrant reconciliation process.

CobiT DS5 *Ensure Systems Integrity, DS 5.3 Identity Management* also suggests that user access rights to systems should be in line with well defined and documented business needs and job requirements.

*Recommendation:*

We recommend that management of the State Treasury Department review QTMS user rights and discontinue any rights that are not necessary for the staff member's normal job functions, and/or those rights which do not support separation of duties. For those cases in which update authority is needed to the warrant files by individuals not usually associated with that function, an administrator could

activate that authority for a limited time basis.

3. The State Treasury Department's Internal Network Should Be Bannered

During our review of the servers of the State Treasury Department, we noted that the systems did not display appropriate network banners. Network banners are electronic messages that provide notice of legal rights to users of computer networks. Bannering assists in the prosecution of computer related incidents by helping prevent certain defenses made by the perpetrator.

*Recommendation:*

We recommend that the State Treasury Department implement appropriate network banners.

4. The State Treasury Department Should Limit Physical Access to Critical Servers

The State Treasury Department has its servers located in a glassed in area on the main department floor. This area has been additionally environmentally secured with automated reporting units that even page the Treasury IT manager on certain events. However, we did note that the server room is not locked, and this presents a physical security risk to the State Treasury Department systems. The *State of Mississippi Enterprise Security Policy* in section XXI Physical Access; Security Guidelines and Recommendations states under Access Control (2) "Smaller computer installations, especially those with critical servers, must be kept in locked rooms. The number of individuals with access to the room must be limited."

*Recommendation:*

We recommend that the State Treasury Department take the additional precaution to always keep its server room locked.