



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

August 1, 2011

Information Systems Management Report

Tom Burnham, Ed.D. Superintendent
Mississippi Department of Education
Mississippi Board of Education
P. O. Box 771
Jackson, Mississippi 39205

Dear Dr. Burnham:

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 Education (MDE). This assessment focused on the adequacy of MDE'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 (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 MDE's Information Systems. Our fieldwork for these assessment procedures was begun on May 12, 2011. 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 limited review of the "Student Information System" application.

Limitations

In planning and performing our limited assessment of MDE's information systems, we considered MDE'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 MDE. Therefore, any exceptions in ITGC are ultimately evaluated as to their impact on financial and federal 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 and corrected on a timely basis. 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 the Mississippi Department of Education did not identify any deficiencies in the general controls that we consider to be a material weakness as defined above. However, we noted five deficiencies in general controls that requires 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 Department of Education 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.

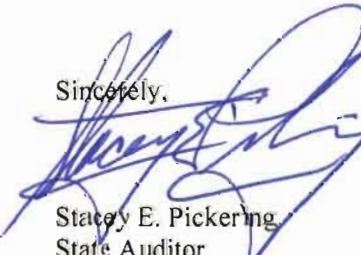
Please review the recommendations included in this report and submit a plan to implement them by, August 23, 2011. The enclosed findings contain more information about our recommendations.

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 Department of Education 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, those charged with Governance, 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 DEPARTMENT OF EDUCATION
AS OF June 16, 2011**

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. User-ids for Separated Employees Were Found in the Current RACF and Active Directory Listings	6
Finding 2. MDE Should Set Expiration Parameters for All Individual's RACF Passwords	6
Finding 3. Access to the Computer Room Should Be Monitored.....	7
Finding 4. Separated Employees Were Found in the Current Oracle Database	7
Finding 5. ORS Needs to Improve Controls over Data Management and Reporting.....	7

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF EDUCATION
AS OF June 16, 2011**

I. ABBREVIATIONS USED IN THIS REPORT

CISA	Certified Information Systems Auditor
DMZ	Demilitarized Zone Configuration Environment
FISCAM	Federal Information Systems Controls Audit Manual
IS	Information Systems
IT	Information Technology
ITGC	Information Technology General Controls
ITS	Mississippi Department of Information Technology Services
MDE	Mississippi State Department of Education
MSIS	Student Information System
ORS	Office of Research and Statistics
OSA	Office of the State Auditor
SAAS	Statewide Automated Accounting System

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF EDUCATION
AS OF June 16, 2011**

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 Department of Education (MDE) to support the integrity and security of the information processed by the computer systems of the MDE at its main office in Jackson, Mississippi. To accomplish these objectives, the Information Systems Audit Section staff of the Office of the State Auditor (OSA):

- Met with MDE management and the OSA financial auditors to gain an understanding of the critical MDE processes and controls;
- Interviewed selected MDE 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 DEPARTMENT OF EDUCATION
AS OF June 16, 2011**

IV. FINDINGS AND RECOMMENDATIONS

CONTROL DEFICIENCIES

1. User-ids for Separated Employees Were Found in the Current RACF and Active Directory Listings

Finding:

Our comparison of the RACF user population against the MDE separated employee list indicated that user-ids for employees on the separated employees list were still listed in RACF and Active Directory.

During the course of the audit MDE removed the user-ids for separated employees from RACF and Active Directory.

COBIT DS5.4 User Account Management includes the following best practice statement, "Perform regular management review of all accounts and related privileges."

Recommendation:

We recommend that MDE continue to monitor and remove terminated employees' user-ids within a short time limit after separation.

2. MDE Should Set Expiration Parameters for All Individual's RACF Passwords.

Finding:

Our review of MDE's RACF security settings identified user-id's with passwords set to never expire. Generally non-expiring passwords should be reserved only for system tasks which could require continuous service. Otherwise all passwords should be set to expire in accordance with policy.

This criteria for best practices in password expiration is established by the Mississippi Department of Information Technology Services in the State of Mississippi Enterprise Security Policy, and is an industry standard security best practice.

Recommendation:

We recommend that all passwords for individual user-ids be set to expire in accordance with the Enterprise Security Policy.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF EDUCATION
AS OF June 16, 2011**

3. Access to the Computer Room Should Be Monitored.

Finding:

Controlled access to sensitive computer room facilities is important to safeguard IT assets and help prevent any disruptions or alterations of computer processing. MDE does have an access card- based zoned door system in place at its headquarters which includes the computer room. However, our review of the access permission list for the computer room facilities revealed that there were some individuals on the list that would have questionable need for direct access into secured computer facilities.

MDE concurred and removed the access of these individuals during the audit.

Recommendation:

We recommend that the MDE MIS Department obtain and review critical area door control listings on a periodic basis. Regular reviews of access which has been granted helps assure that the minimum number of individuals have access to the secure computer room.

4. User-ids for Separated Employees Were Found in the Current Oracle Database.

Finding:

Our review of the Oracle database found user-ids for separated employees in the current Oracle database.

During the course of the audit MDE removed the identified separated employees from the Oracle database.

COBIT DS5.4 User Account Management includes the following best practice statement, "Perform regular management review of all accounts and related privileges."

Recommendation:

We recommend that MDE continue to monitor and remove terminated employees' user-ids within a short time limit after separation

5. ORS Needs to Improve Controls over Data Management and Reporting.

Finding:

The ORS department produces reports and gathers information for various people and organizations both internal and external to MDE. ORS gathers some information directly and the rest comes from the MSIS application maintained by MDE MIS department. The ORS department is operating outside the MDE MIS department and therefore does not conform to the policies and procedures set forth by MDE

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF EDUCATION
AS OF June 16, 2011**

MIS. During an interview with ORS personnel several issues concerning data management and reporting procedures were noted by OSA. If ORS is to continue to operate in this manner, the following deficiencies need to be addressed to comply with best practices as well as sections of the Enterprise Security Policy to which all agencies must adhere:

- Data is being stored on PCs, one of which appears to be a laptop.
- PCs are not being backed up.
- There is no disaster contingency plan in place for ORS.
- There are no formal change control policies in place.
- There are limited edits to insure the integrity of the data or reports.
- There is limited documentation for the department.

Recommendation:

We recommend ORS adhere to fundamental controls and policies to protect data entrusted to their care. ORS needs to develop a formal set of policies and procedures to govern the handling of the data and the creation of the reports.

End of Report



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

*Original letter
 sent to the below
 listed members, also.*

August 1, 2011

Information Systems Management Report

Claude Hartley, Member
 Mississippi Board of Education
 4437 Ridgeway Drive
 Belden, Mississippi 38826

Howell N. Cage, Member
 Mississippi Board of Education
 1400 Highway 61 North Bypass
 Vicksburg, Mississippi 39183

Dear Mr. Hartley:

Aug

Info:

Information Syst

Kami Bumgarner, Member
 Mississippi Board of Education
 1365 Mannsdale Road
 Madison, Mississippi 39110

William Harold Jones, Member
 Mississippi Board of Education
 P.O. Box 282
 Petal, Mississippi 39465

Dear Mrs. Bumgarner:

Dear Mr. Jones:

Aug

Infor

Information Syste

Martha Murphy, Member
 Mississippi Board of Education
 57 Cr. 8050
 Rienzi, Mississippi 38865

Dr. Sue Matheson, Member
 Mississippi Board of Education
 6457 Kiln Delisle Road
 Pass Christian, Mississippi 39571

Dear Mrs. Murphy:

Dear Dr. Matheson:

Aug

Infor

Information Syste

Charles McClelland, Member
 Mississippi Board of Education
 6252 Winthrop Circle
 Jackson, Mississippi 39206

Dr. O. Wayne Gann, Member
 Mississippi Board of Education
 109 Dunbar Avenue
 Corinth, Mississippi 38834

Dear Mr. McClelland:

Dear Dr. Gann: