STATE OF MISSISSIPPI

OFFICE OF THE STATE AUDITOR
STACEY E. PICKERING
STATE AUDITOR

March 25, 2015

Information Systems Management Report

Craig P. Orgeron, Ph.D., Executive Director
Mississippi Department of Information Technology Services
3771 Eastwood Drive
Jackson, Mississippi 39211 - 6381

Dear Dr. Orgeron:

The Office of the State Auditor has completed its limited assessment of the Information Systems (IS) general controls of the Mississippi Department of Information Technology Services (ITS). This assessment focused on the adequacy of the ITS'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: 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 ITS'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 ITS's information systems, we considered ITS'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 financial audit of the State of Mississippi. 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 Information Technology Services 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 deficiencies involving 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 April 10, 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 ITS'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 ITS 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 INFORMATION TECHNOLOGY SERVICES
AS OF NOVEMBER 21, 2014

TABLE OF CONTENTS

OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT of INFORMATION TECHNOLOGY SERVICES
AS OF NOVEMBER 21, 2014

I. ABBREVIATIONS USED IN THIS REPORT

APT	Advanced Persistent Threat
FISCAM	Federal Information Systems Controls Audit Manual
HIPAA	Health Insurance Portability and Accountability Act
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

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 Information Technology Services to support the integrity and security of the information processed by the computer systems of ITS 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 Mississippi Department of Information Technology Services management to gain an understanding of the critical Mississippi Department of Information Technology Services' processes and controls;
- Interviewed selected Mississippi Department of Information Technology Services' technology 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.

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. 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

CONTROL DEFICIENCIES

1. Agency-level Efforts for Threat Reduction Should Be Expanded.

Finding:

Condition

The Mississippi Department of Information Technology Services (ITS) manages Enterprise State Network and State Data Center solutions in order to maintain a shared and trusted environment for its clients which include state agencies, institutions of higher learning and state medical facilities. ITS currently uses individual products to ensure the availability and protection of the infrastructure that supports the services offered to their clients. The use of these products requires considerable manual monitoring and absorbs a considerable amount of the agency's limited staff resources.

Recently, data breaches worldwide have occurred more frequently as well as have become more sophisticated and more damaging. The degree of planning, resources employed and techniques used in carrying out such attacks is unprecedented. Government entities are common victims because of the large amounts of sensitive data that they store.

The cybersecurity threat landscape is constantly changing and evolving. These threats demand a set of countermeasures that are above and beyond those routinely used to counter everyday security threats. As cyber threats have evolved so have the tools to combat these types of attacks.

As a necessary part of doing business, entities such as the State of Mississippi are becoming increasingly dependent on digital technologies. As cyberattacks become more sophisticated and new technologies develop, the risk of unauthorized access to data assets increases.

The impact of a successful cyber-attack on any entity could lead to severe damages. These damages can be in the form of fines, future liabilities, missed economic opportunities and security threats.

Recommendation:

The Department of Information Technology Services' current efforts are primarily focused on enterprise-wide threat reduction. We recommend that ITS continue to expand these efforts to better reduce threats to ITS-specific systems by continuing to implement core security functions for managing cybersecurity risk. The goal should be to ensure an agency-wide proactive effort to prevent, detect and respond to emerging cyber threats with minimal ad-hoc intervention.

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

Finding:

Mississippi Department of Information Technology Services (ITS) 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. While the IT related policies and procedures that do exist for ITS are well prepared and understandable, there are some areas which are not adequately covered in these policies and procedures that should be of great concern to an organization the size, complexity and importance of ITS. These areas include:

- Data Breach Management;
- Encryption;
- Physical and Logical Access Reviews;
- HIPAA.

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."

Policies and procedures must be looked at by management as guidelines from which management decisions are made and for the day to day actions of employees. Policies and Procedures 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. Policies and procedures must be looked at by management as documents that change to fit the business environment yet rigid enough to give general direction for decisions. This need for change has no better example than the area of technology where development of new technologies as well as changes in existing technologies cause frequent changes in the business environment.

Not having formal policies that adequately cover all areas that are pertinent to the organization causes confusion for 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:

Existing policies and procedures should be changed to more adequately cover:

- Data Breach management;
- Encryption (data at rest, data in transit, emails, and portable devices);
- Formal access reviews;
- HIPAA.

Policies that are specific to detail regulations such as HIPAA should be segregated from general IT policies and procedures as this can help employees to better understand their responsibilities and therefore be more likely to comply with guidelines and regulations that can greatly affect the financial stability and reputation of an organization.

Also, 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.

End of Report