STATE OF MISSISSIPPI

OFFICE OF THE STATE AUDITOR
STACEY E. PICKERING
STATE AUDITOR

September 24, 2013

Information Systems Management Report

Members of the Board of Supervisors
Madison County, Mississippi
125 West North Street
Canton, Mississippi 39046

Dear Board Members:

The Office of the State Auditor has completed its limited assessment of the Information Systems (IS) general controls of Madison County, Mississippi ("the County"). This assessment focused on the adequacy of Madison County'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 financial and compliance audit of Madison County, 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), LaDonna Johnson, MBA, CISA (Senior IS Auditor).

Scope of Our Review

To support our general controls assessment, our procedures were performed through observations and discussions of the information technology general controls (ITGC) of Madison County's Information Systems. Our fieldwork for these assessment procedures was begun on May 22, 2013. 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 Madison County's information systems, we considered Madison County's (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 financial and compliance audit of Madison County. 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 in 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 control 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 deficiencies, 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 Madison County's Information Systems identified significant deficiencies in the internal control over IS and a control deficiency, as defined above. Additionally, we noted certain deficiencies involving internal control over ITGC that require the attention of management. These matters are noted under the headings SIGNIFICANT DEFICIENCIES AND CONTROL DEFICIENCY in Internal Control respectively. As part of obtaining reasonable assurance about whether selected IS general controls of Madison County are functioning as designed, we performed assessments of compliance with certain regulations and industry best practices. However, 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, October 25, 2013. 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 Madison County throughout this review. If you have any questions or need more information, please contact me.

This report is intended solely for the information and use of management, individuals charged with governance, others within the entity, federal awarding agencies and pass-through entities 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,

Patrick Dendy, CPA
Director, Department of Audit

Enclosures

OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MADISON COUNTY, MISSISSIPPI
AS OF SEPTEMBER 24, 2013

TABLE OF CONTENTS

Page No.

SIGNIFICANT DEFICIENCIES IN INTERNAL CONTROL

CONTROL DEFICIENCY

OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MADISON COUNTY, MISSISSIPPI
AS OF SEPTEMBER 24, 2013

I. ABBREVIATIONS USED IN THIS REPORT

CobiT	Control Objectives for Information and Related Technology
ESP	Enterprise Security Policy
IS	Information Systems
IT	Information Technology
ITGC	Information Technology General Controls
ITS	Mississippi Department of Information Technology Services
LAN	Local Area Network
OSA	Office of the State Auditor
PCs	Personal Computers
The County	Madison County, Mississippi
WAN	Wide Area Network

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 Madison County to support the integrity and security of the information processed by the computer systems of Madison County at its courthouse in Canton, Mississippi. To accomplish these objectives, the Information Systems Audit Section staff of the Office of the State Auditor (OSA):

- Met with Madison County and the OSA auditors to gain an understanding of the critical Madison County processes and controls;
- Interviewed selected Madison County 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.

IV. FINDINGS AND RECOMMENDATIONS

SIGNIFICANT DEFICIENCIES

1. Madison County Should Establish and Test a Formal Disaster Recovery Process

Finding:

During our review of the IS controls of Madison County, we noted that the County has not established a disaster recovery process including a complete plan and documented test of this plan. As a result, Madison County cannot fully ensure that the county's information systems can be restored in a timely manner. Disaster recovery involves defining and documenting plans to help sustain and recover critical information technology resources, information systems, and associated business functions. *Control Objectives for Information and Related Technology* (CobiT, Section DS4), as well as recognized industry best practices, require a written disaster recovery plan be developed and tested regularly to provide orderly recovery of vital functions in the event of a hardware or environmental disaster. Failure to maintain an adequate recovery plan could impede the agency's ability to regain computer operations in the event of a disaster.

There are a number of steps that an organization can take to prevent or minimize the damage to automated operations that may occur from unexpected events. An example is routinely verifying the veracity of back up medium as a part of the process of conducting a formal, documented test of the recoverability of critical systems in a timely manner. This should be done periodically (at least annually) as a part of a formal, documented disaster recovery exercise. Such actions maintain the organization's ability to restore data files, which may be impossible to re-create.

Madison County is currently using an automated system to perform daily back-ups of the AS400, but is not restoring such files as part of a formal, documented disaster recovery exercise. Without proper assurance that back-up files can be utilized to adequately restore all critical data in a timely manner in the event of a disaster scenario, material damage could be realized by the County and its processes should a catastrophic event occur involving the County's building, servers, and staff. Risk and probabilities of material loss escalates in relationship to the longer an exposure goes unmitigated.

Recommendation:

We recommend that Madison County develop, implement, and conduct a documented test of its plan to insure that critical data and applications are recoverable in case of a disaster scenario. We further recommend that Madison County develop and implement a disaster recovery plan documenting procedures to be followed during an emergency. Once the plan is completed, it should be subjected to proper testing, and employees should be made aware of their responsibilities in the event of a disaster. The plan should be updated when needed in order to maintain readiness for a disaster scenario.

2. Madison County Needs to Replace Obsolete Computer Hardware and Software.

Finding:

Madison County is running operating systems as well as the applications on many of its personal computers (PCs) that might not be supported by vendors. Due to lack of such support, these systems could become vulnerable to hackers and malware such as viruses.

Recommendation:

We recommend that Madison County develop a plan to replace the operating systems, applications, and hardware where necessary that is associated with lack of support from vendors as soon as possible. Computers that originally came loaded with operating systems or applications that are no longer supported by vendors will have hardware that most likely cannot run the newest operating systems or applications, thereby requiring replacement of hardware, operating systems and applications in many cases. Due to the rather large number of PCs that possibly need replacing this could involve a sizable expenditure by the County. Due to the cost and effort involved in such a project, this project should be begun as soon as possible.

3. Madison County Should Implement a Formal Information Security Policy.

Finding:

Madison County has not adopted a formal Information Security Policy or Enterprise Security Plan. The lack of a formal Information Security Policy can lead to a breakdown of basic security practices in the areas of application security, LAN/WAN security, management of the security application and Internet protocol.

Recommendation:

While full compliance with all facets of a robust Information Security Policy may be an economic challenge for Madison County, beginning steps to become compliant with such are necessary. We recommend that Madison County create a plan of compliance with industry standards to ensure progress towards a robust documented information security plan. This policy should be reviewed and approved by county supervisors. In addition, employees that utilize technology should review and accept such policies before access to computer resources is granted to employees. Proof of approval by management and acceptance by employees should be retained for review by auditors.

4. Madison County Should Encrypt Laptops and Other Portable Devices Containing Sensitive Information.

Finding:

Madison County is not using encryption where appropriate. Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail.

Recommendation:

Madison County should define what data they consider to be sensitive and begin to protect this data appropriately, especially on laptops or other portable devices currently being used by county personnel to insure that they comply with House Bill 583 (Mississippi State Data Breach Law) which states: For purposes of this section, the following terms shall have the meanings ascribed unless the context clearly requires otherwise:

(a) *"Breach of security" means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.*

V. Control Deficiency

5. Madison County Should Expire All Individual's Passwords on a Periodic Basis.

Finding:

A review of Madison County's security settings revealed that some user's passwords were set to expire on a more infrequent basis then recommended in best business practices. All passwords should be set to expire in accordance with policy to be determined by Madison County.

Recommendation:

We recommend that a policy be implemented to insure passwords are expired on a regular basis.

6. Password Strength Should Be Improved.

Finding:

During our review, we noted that Madison County is using a password length of 6 characters on its AS400, along with a required password change every 90 days. Industry standard and best practices set the minimum length to be at least 8 characters.

Recommendation:

We recommend that Madison County improve its password length to comply with password management best practices and industry standards.

End of Report

MADISON COUNTY BOARD OF SUPERVISORS

125 West North Street • Post Office Box 608
Canton, Mississippi 39046
601-855-5500 • Facsimile 601-855-5759
www.madison-co.com

November 12, 2013

INFORMATION SYSTEMS MANAGEMENT REPORT

Honorable Stacey E. Pickering, State Auditor
Office of the State Auditor
State of Mississippi
PO Box 956
Jackson, MS 39205-0956

Dear Mr. Pickering:

We have received your report of your limited assessment of the Information Systems (IS) controls of Madison County. Please find a summary of your findings and the county's responses below.

Finding 1: Madison County should establish and test a disaster recovery process.

Response: Madison County agrees with this finding in regard to a catastrophic disaster.

Madison County has procedures in place to backup up its data on all platforms. The media, on which this backup is written to, is stored at an off-site facility. This facility is a sufficient distance from our operations to provide reasonable safety of the backup media. The facility is operated by a reputable third-party provider.

The backup media is picked up daily and delivered to this facility, which is an environmentally controlled and protected environment. The media is stored until the date of its scheduled return to the IT Department to be used in the next backup rotation. The media is rotated on a schedule where there are 8 sets of daily backups (Monday through Thursday), for a two week daily rotation. There are 4 sets of weekly backups (Friday of each week) for a 4 week rotation. There are 6 sets of monthly backups done on the last day of each month for a 6 month rotation. A review is performed each day of the backup jobs and associated logs to verify completeness of the backup.

The assurance that the data is complete is confirmed by the fact that this same backup media has been used multiple times to restore all data onto a new system when we have implemented system upgrades. In addition, the IT department periodically receives requests to restore data from the backup media. These restorations are performed with no problems detected.

The above information only addresses the backups and integrity of the data on the backup media. It does not address the fact that there is no equipment to restore the data to in the event of a major disaster (i.e. building fire, tornado, etc.) that would destroy the actual hardware that the data resides on for production access.

Madison County will research the cost associated with securing an off-site facility that would allow the county to quickly resume operation of computer systems to support daily county activities. This task is assigned to the IT Director.

Finding 2: Madison County needs to replace obsolete computer hardware and software.

Response: Madison County agrees with this finding.

Resources have been included in the current county budget to fund replacement of this equipment and software.

A private vendor and the IT Department are currently replacing the obsolete equipment and software.

Finding 3: Madison County should implement a formal information security policy.

Response: Madison County agrees with this finding.

Although not formalized into a policy statement, Madison County has security practices in place. All systems and servers are password protected. All outside network access is protected by a security appliance that requires a VPN client with a security profile and network log-on credentials in order to access the network from outside. The internal wireless network is protected by a lengthy encryption key that is required to connect to the internal wireless network.

An IT policy is included in the employee handbook. This IT policy will be reviewed and modified, if needed, to address specific security policies.

The County Administrator and IT Director, in cooperation with the Board Attorney, will review policies to propose any necessary updates to the Board of Supervisors.

Finding 4: Madison County should encrypt laptops and other portable devices containing sensitive data.

Response: Madison County agrees with this finding, when a device contains confidential data.

The laptops and portable devices in Madison County are primarily utilized to connect to the internal network. This connection occurs through a secure VPN client, requiring a pre-authorized profile and the employee's network credentials. The employee then accesses data on internal file servers and desktops. This does not cause sensitive files to be downloaded to the portable computer.

A review by the IT Director will be conducted to verify the security of data on laptops and portable devices.

Finding 5: Madison County should expire all individual passwords on a periodic basis.

Response: User profiles will be reviewed by the IT department and necessary adjustments will be made to cause passwords to expire on appropriate profiles on a periodic basis.

The IT Director will oversee this review.

Finding 6: Password strength should be improved.

Response: Madison County agrees with this finding.

Madison County will review industry standards and make appropriate changes, after sufficient notification is given to the end-user community.

The IT Director will perform this task.

After review of the county's responses, if you determine that additional information is required, please advise the interim County Administrator Shelton Vance at 601-855-5502.

Sincerely,

Gerald Steen,
Board President