AUDITOR GENERAL

WILLIAM O. MONROE, CPA

POLK COUNTY DISTRICT SCHOOL BOARD

Information Technology Audit

SUMMARY

The Polk County District School Board (District) maintains SAP enterprise resource planning (ERP) software that provides application processing for District administrative systems, such as general ledger, accounts payable, human resources, and payroll functions. Our audit focused on evaluating management controls and selected information technology (IT) functions applicable to the SAP system during the period October 2003 through January 2004, with selected actions taken through February 2004, including selected general controls; determining management's awareness of, and actions taken regarding, the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and determining whether the District has corrected, or is in the process of correcting, IT-related deficiencies disclosed by the predecessor auditor in a management letter dated April 17, 2003.

Certain deficiencies were noted in the District's management controls over selected IT functions. Specifically, these deficiencies included:

Finding No. 1: Improvements were needed in the District's systems modification methodology.

Finding No. 2: Improvements were needed in the District's IT risk management practices.

Finding No. 3: System access privileges were not, in some instances, restrictive enough to enforce a proper segregation of incompatible duties.

Finding No. 4: Deficiencies were noted in the District's IT security controls in addition to the matters discussed in Finding No. 3.

Finding No. 5: Deficiencies were noted in the District's business continuity controls.

BACKGROUND

SAP ERP software was operated in a client-server environment under the management of the Information Systems and Technology division.

Information Systems and Technology was responsible for providing IT resources to meet the needs of the District. Electronic Equipment

Repair and Support, Systems and Applications, Computer Networking, Data Processing, School Technology Service, and Information Systems were functional areas that reported to the Senior Director, Information Systems and Technology.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Systems Modification Methodology

A proper systems modification methodology documents management's expectations in such areas as requests for modifications, coding and testing, review and approval, user acceptance, and promotion of modifications to production.

The District had implemented a change management process to track and document the requesting, coding, and testing of SAP system modifications by programmers and the requests for business analysts to transport those changes to test and production. However, the form used to track modifications made by the programmers and the form used to request transport of those changes by the business analysts were not tied together by a common identifier. Consequently, the ability did not exist to efficiently track the progress of the change from the initial request through the promotion of the change into production or to trace production program changes back to supporting authorization documents. Also, user testing and acceptance of changes, if performed, were not documented.

Additionally, some new or modified queries and reports were created by business analysts rather than programmers. Since the business analysts were not required to complete the same form that programmers completed for program modifications, there was no change management process to track and document the reports and queries created by the business analysts.

These conditions increase the risk that incorrect program modifications, including reports and queries, may be placed into production, jeopardizing the accuracy of reporting for decision making purposes.

Recommendation: The District should improve its systems modification methodology to define when user testing and acceptance are required, address all report and query creations and modifications, and ensure the ability to efficiently track program changes. Within the methodology, documentation requirements should facilitate the identification of the user(s) who submitted a programming or report request and tested and approved the change.

Finding No. 2: IT Risk Management

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization, and its ability to perform its mission, from IT-related risk. The risk management process involves identifying and assessing risk, and taking steps to reduce risk to an acceptable level.

We noted deficiencies in the District's IT risk management practices. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising District information. However, the appropriate personnel have been notified of the deficiencies.

Recommendation: The District should implement the appropriate IT risk management practices to provide increased assurance that IT-related risks are identified and managed in a cost-effective manner.

Finding No. 3:
System Access Privileges

Segregation of incompatible duties is fundamental to the reliability of the organization's internal controls. Appropriate segregation of duties can assist in the detection of mistakes or errors and potential fraud. Access to processing functions should be controlled in a manner that permits authorized users to gain access only for purposes of performing their assigned duties. Whenever practicable, one person should not control all stages of a process, to minimize the likelihood that errors or fraud could occur without detection.

We noted instances of questionable employee access privileges that should be made more restrictive by the District to enforce an appropriate segregation of duties. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, the appropriate personnel have been notified of the issues.

Recommendation: The District should review the duties and access capabilities of the District staff and implement a proper segregation of duties to the extent practicable.

Finding No. 4:
Security Control Deficiencies

Security controls are intended to protect the integrity, confidentiality, and availability of information systems data and resources.

We identified deficiencies in certain District security control features in addition to the matters discussed in Finding No. 3. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising District information. However, the appropriate personnel have been notified of the deficiencies.

Without adequate security controls in place, the risk is increased that the District's information resources may be subject to improper disclosure.

Recommendation: The District should implement the appropriate security control features to enhance the security over the District's data and programs.

Finding No. 5: Business Continuity Controls

Business continuity controls are intended to ensure continuous service to meet District business requirements, make certain IT services are available as required, and lessen the business impact in the event of a major disruption. Business continuity planning identifies and provides information on supporting resources needed and the roles and responsibilities of those involved in the recovery process, including user department personnel.

We identified deficiencies in the District's business continuity controls. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of the deficiencies.

Recommendation: The District should enhance its business continuity controls.

OTHER MATTERS

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA[1] addresses data interchange, privacy, and information security standards for personal health information. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards, privacy, and security. The final Transaction Rule, which contains electronic data interchange standards, was incorporated as a Federal regulation and had a compliance date of October 16, 2002. The final Privacy Rule was incorporated as a Federal regulation and compliance was required by April 14, 2003. The final Security Rule was incorporated as a Federal regulation and has a compliance date of April 21, 2005. HIPAA also provides for civil and criminal penalties for noncompliance. Management had determined that the District falls under current provisions of HIPAA and had instituted security measures relating to specific provisions of the Privacy Rule. Additionally, the District stated that applicable vendors under contract with the District were responsible for following the Transaction Rule. The District should continue to evaluate the impact of HIPAA requirements on all District IT activities due to the dynamic nature of the data transmitted over the network which may be subject to this Act in the future.

PRIOR AUDIT FINDINGS

Except as discussed in the preceding paragraphs, the District had corrected, or was in the process of correcting, portions of the IT-related deficiencies as reported by the predecessor auditor. Certain issues within Finding Nos. 2 and 4, previously noted by the predecessor auditor, remained unresolved.

[1] Public Law 104-191

SCOPE, OBJECTIVES, AND METHODOLOGY

The scope of this audit focused on evaluating management controls and selected IT functions applicable to the SAP system during the period October 2003 through January 2004, with selected actions taken through February 2004. Our objectives were to determine the effectiveness of selected IT controls; to determine management's awareness of and actions taken regarding HIPAA; and to determine whether the District had corrected, or was in the process of correcting, IT-related deficiencies disclosed by the predecessor auditor in a management letter dated April 17, 2003.

In conducting our audit, we interviewed appropriate District personnel, observed District processes and procedures, and performed various other audit procedures to test selected IT controls.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

DISTRICT'S RESPONSE

In a letter dated May 3, 2004, the Superintendent provided responses to our preliminary and tentative findings. This letter is included in its entirety at the end of this report.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Stephanie Hogg, CISA, and supervised by Nancy Reeder, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.state.fl.us/audgen); by telephone (850 487 9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.

SCHOOL BOARD OF POLK COUNTY

P.O. BOX 391
BARTOW, FLORIDA 33831

1915 SOUTH FLORAL AVENUE
BARTOW, FLORIDA 33830

(863)-534-0500 • SUNCOM 549-0500 • FAX (941)-534-0705

May 3, 2004

William O. Monroe, CPA
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe,

We are in receipt of your preliminary and tentative audit findings and recommendations dated April 1, 2004. Our response regarding each of the findings follows.

Finding No. 1: Systems Modification Methodology
The District has improved its system modification methodology as described in the recommendation. The change request form has been changed to provide a place for user sign-off to indicate user testing and acceptance, as well as identification of the user who submitted the request and the original Data Processing Programming Request number. In addition, Data Processing Programming Requests are now required for all report and query creations and modifications.

Finding No. 2: IT Risk Management
The District is implementing, to the extent practicable, the appropriate IT risk management practices to provide increased assurance that IT-related risks are identified and managed in a cost-effective manner, and the District is in the process of implementing more comprehensive IT Security Policies and Procedures. Some of the specific recommendations outlined in the audit cannot be fully addressed due to limited District resources. Specific details of the District's response to this finding are not disclosed to avoid the possibility of compromising District information.

Finding No. 3: System Access Privileges
The District is reviewing the duties and access capabilities of staff and implementing a proper segregation of duties to the extent practicable, and the District is in the process of implementing more comprehensive IT Security Policies and Procedures. Some of the specific recommendations outlined in the

May 3, 2004 – Page 2

audit cannot be fully addressed due to limited District resources. Specific details of the District's response to this finding are not disclosed to avoid the possibility of compromising District information.

Finding No. 4: Security Control Deficiencies
The District is implementing the appropriate security control features to the extent practicable to enhance security over the District's data and programs, and the District is in the process of implementing more comprehensive IT Security Policies and Procedures. Some of the specific recommendations outlined in the audit cannot be fully addressed due to limited District resources. Specific details of the District's response to this finding are not disclosed to avoid the possibility of compromising District information.

Finding No. 5: Business Continuity Controls
The District is enhancing most of its business continuity controls as recommended. Some of the specific recommendations outlined in the audit cannot be fully addressed due to limited District resources. Specific details of the District's response to this finding are not disclosed to avoid the possibility of compromising District information.

We appreciate the professional and courteous manner in which your staff conducted this audit, and thank you for the opportunity to improve the Information Technology practices in our District.

Sincerely,

R. J. Thornhill
Superintendent