



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



ST. JOHNS COUNTY

DISTRICT SCHOOL BOARD

Information Technology Audit

SUMMARY

The St. Johns County District School Board (District) utilizes Oracle-based applications and databases to manage its financial resources. Our audit focused on evaluating selected information technology (IT) controls applicable to the Oracle financials application and surrounding infrastructure during the period July 2005 through June 2006 and selected actions taken through November 2006.

As described below, we noted that improvements were needed in certain controls related to the District’s IT functions and practices.

Finding No. 1: User access capabilities in the Oracle application were, in some instances, inappropriate, excessive, unsupported by written authorization, or inconsistent with what was authorized in writing.

Finding No. 2: The District’s Information Technology Procedures Handbook lacked certain important security policies and procedures.

Finding No. 3: Improvements were needed in certain security controls protecting the Oracle financials application and surrounding IT infrastructure.

BACKGROUND

The District purchased and began implementation in 2000 of the Oracle-based applications and databases. Oracle 11i eBusiness Suite was the database and application software used by the District to consolidate human resources, payroll, and finance-related information into a comprehensive systems management environment.

As of April 2006, the District served a population of 25,248 students and employed 3,002 faculty and staff. Students, faculty, and staff relied on the District’s IT infrastructure and services to accomplish their assigned tasks. IT services were considered a critical component in the daily operations of the District. The IT Department was under the direction of the District’s Chief Information and Technology Officer, who reported directly to the Superintendent, and it consisted of the following areas: Network Services; Technology Support; Oracle Database Administration; and Oracle/eSIS Applications.

**Finding No. 1:
Authorization of Access**

Good IT security practices dictate that access authorizations be documented on standard forms, maintained on file, approved by management, and communicated to security managers. According to the District’s IT Procedures Handbook, the Finance and Human Resource department heads or designees were to submit to the computer operator or application database administrator Oracle application login requests for system access and role responsibilities.

During our audit, we requested evidence to support Oracle application user access privileges for 13 employees. We noted the following:

- Documentation of authorized access capabilities did not exist for 4 of 13 employees tested.

- For 4 of the 9 employees for whom documentation existed, the access capabilities granted did not match the authorized level of access.

Our audit also disclosed instances of inappropriate or excessive access privileges. An appropriate division of roles and responsibilities excludes the possibility of a single individual subverting a critical process. When enforced through appropriate system access privileges, such a division helps ensure that personnel are performing only those duties stipulated for their respective jobs and positions. During our testing of end-user and IT staff access privileges, we noted the following:

- Twenty-seven of 34 end-users appeared to have inappropriate or excessive access privileges to Oracle application responsibilities. Twenty-six of the 27 end-users had human resources management system access privileges, which allowed them to add and update employees, as well as set up payroll. Thirteen of these 26 end-users also had access privileges that inappropriately allowed them the ability to define and assign security profiles. In response to our audit inquiry, District staff indicated that these access privileges were under review.
- Six of 12 IT staff tested appeared to have excessive end-user update privileges assigned to their user IDs.

Subsequent to our audit inquiries, District staff indicated that they were in the process of customizing and establishing specific roles and privileges to better match each job position and to minimize users from accessing areas that were not a part of their job function.

Absent an appropriate segregation of duties, the risk is increased that erroneous or fraudulent transactions could be processed. Further, failure to document access authorizations increases the risk of inappropriate access and unauthorized use, disclosure, or modification of data and programs.

Recommendation: In order to preserve the integrity, confidentiality, and availability of its information resources, the District should strengthen access authorization controls in the above-listed areas. Specifically, users' roles should be reviewed to ensure that they are reflective of the job duties of the individual to whom they are assigned.

Finding No. 2:

IT Standard Operating Procedures

Each function in an organization needs complete, well-documented policies and procedures to describe the scope of the function, its activities, and the interrelationships with other departments. District staff had developed an IT Procedures Handbook that documented the guidelines, rules, requirements, and actions affecting IT services at St. Johns County Schools. Although the Handbook identified activities, resources, and procedures necessary to carry out IT activities during daily operations, the Handbook lacked written policies and procedures for the following activities being performed by the District:

- Periodic review of the appropriateness of Oracle application users' access rights.
- The update or removal of Oracle user accounts as a result of employee terminations or transfers.
- Change control for upgrades and patches to the network, operating system, and database.
- Reporting of and response to security incidents involving privacy violations.

Subsequent to our audit inquiries, District staff provided an updated version of the Handbook that included procedures for the periodic review of Oracle user accounts and described procedures being implemented for modifying and removing user accounts using reports from the Oracle human resources application. The updated Handbook also partially addressed reporting and response regarding security incidents.

The absence of written policies and procedures increases the risk that sound information security controls will not be consistently applied as intended by

management to prevent the compromise of data confidentiality, integrity, and availability.

Recommendation: The District should continue to establish written policies and procedures for the aforementioned functions within the IT Department. Once established, the policies and procedures should be periodically reviewed and updated for all relevant changes.

Finding No. 3:

Other Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of data and IT resources. During our audit, we identified certain security control deficiencies related to controls over the network, operating system, and database, in addition to the matters previously discussed in this report. Specific details of the security control deficiencies are not disclosed in this report to avoid the possibility of compromising the District's information and resources. However, appropriate District staff have been notified of the deficiencies. Without adequate security control features in place, the risk is increased that the District's information resources may be subject to improper disclosure, destruction, modification, or undue disruption.

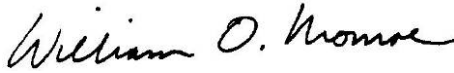
Recommendation: The District should implement stronger security controls to further protect the District's data and IT resources from misuse.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected District IT controls. Our scope focused on selected general and application IT controls relevant to the Oracle financials application and the surrounding technology infrastructure during the period July 2005 through June 2006 and selected actions taken through November 2006. In conducting our audit, we interviewed appropriate District personnel, reviewed District processes and procedures, and performed various other audit procedures to test selected 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, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated March 9, 2007, the Superintendent provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

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 conducted in accordance with applicable Generally Accepted Government Auditing Standards. This audit was conducted by Kathy Sellers, 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.

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX A
MANAGEMENT RESPONSE

St. Johns County School District
40 Orange Street
St. Augustine, Florida 32084
(904) 819-7500
www.stjohns.k12.fl.us
Joseph G. Joyner, Ed.D.
Superintendent



March 9, 2007

William O. Monroe
Office of the Auditor General
State of Florida
G-74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe,

Attached is the District response to the Preliminary and Tentative findings for the Information Technology Audit of the St. Johns County School District for the period of July 2005 through June 2006.

Sincerely,

Joseph G. Joyner, Ed.D.
Superintendent of Schools

/mh

Attach.

The St. Johns County School District will inspire in all students a passion for lifelong learning, creating educated and caring contributors to the world.

School Board

Beverly Slough
District 1

Tommy Allen
District 2

Bill Mignon
District 3

Bill Fehling
District 4

Carla Wright
District 5

Information Technology Auditor General's Finding No. 1: Authorization of Access

District Response: The District will strengthen Oracle access authorization controls and review the roles (and privileges) of existing users. It is expected that many roles will be streamlined (or customized) to better match each user's job function and responsibility.

Information Technology Auditor General's Finding No. 2: IT Standard Operating Procedures

District Response: The District will continue to strengthen and expand its written information technology procedures in the areas noted and review them periodically making changes as needed.

Information Technology Auditor General's Finding No. 3: Other Security Controls

District Response: The District will review, research and implement stronger security controls noted in the audit (where appropriate).

THIS PAGE IS INTENTIONALLY LEFT BLANK