



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



ORANGE COUNTY

DISTRICT SCHOOL BOARD

Information Technology Audit

SUMMARY

The Orange County District School Board (District) maintains SAP America Public Sector, Inc. (SAP) enterprise resource planning (ERP) software to support various administrative functions. Our audit focused on evaluating selected information technology (IT) controls applicable to the SAP financials application and surrounding infrastructure during the period July 2006 through June 2007 and determining whether the District had corrected, or was in the process of correcting, IT-related deficiencies disclosed in audit report No. 2005-109 and by the predecessor auditor in its management letter dated October 20, 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: Improvements were needed in the District’s IT security management.

Finding No. 2: Deficiencies were noted in the District’s disaster recovery plan and process.

Finding No. 3: Improvements were needed in off-site backup procedures.

BACKGROUND

The implementation of SAP software in July 1999 provided application processing for the District’s administrative systems, such as general ledger, accounts payable, purchasing, personnel, and payroll functions. The District upgraded its SAP system in July 2005. The SAP application runs on an AIX operating system and uses Oracle as the database management system.

Information, Communications, and Technology Services (ICTS) is a district-level department that provides an integrated set of automated processes and support to meet the administrative and operational needs of the District. ICTS maintains and operates the SAP financials system. 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 ICTS department was under the direction of the District’s Chief Information Officer, who reported directly to the Chief Operations Officer. The ICTS organizational structure consists of the following areas: Applications, Infrastructure, Customer Care, Field Services, and Enterprise Project Office.

**Finding No. 1:
Security Management**

Effective security relies on a security structure that includes consideration of data classification and ownership, organizational and operational policies, a thorough review of security, and security administration procedures. Specific procedures developed and documented for each of the major functions of security administration include the design of the security hierarchy; the granting and revoking of data and resource access; and the reporting and monitoring of activity.

There were aspects of the District's security management that needed improvement. Specifically:

- Management had not established policies and procedures for the periodic review of user access rights for the SAP application, nor had it performed periodic reviews.
- Certain important security features available in the software had not been utilized, and certain security controls protecting the network, operating system, database, and the administrative applications were inadequate. Specific details of these security deficiencies are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of these deficiencies.
- The District had an automated process in place to ensure the timely deletion of terminated accounts, processing of inactive accounts, and maintenance of the list of current users and their associated accounts. However, the District's written policies and procedures had not been updated to coincide with the automated process.
- The District's monitoring of system security events and activity needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of these issues.
- Certain District staff had the capability to perform incompatible duties. Separation of incompatible duties is fundamental to the reliability of an organization's internal controls. Appropriate separation of duties can assist in the prevention and detection of mistakes or errors and potential fraud. 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 separation of duties. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate personnel have been notified of these issues.

Absent sound security management, the risk is increased that information security controls will not be sufficiently assessed and imposed to prevent compromise of data confidentiality, integrity, and availability.

Recommendation: The District should implement a plan to ensure that policies and procedures are in place for security-related functions within the organization. The policies and procedures should be reviewed periodically and updated as needed for organizational and system-related changes to help ensure that management requirements are met by District staff when performing assigned tasks. Also, the District should implement appropriate security control features to enhance security over its data and programs. Furthermore, the District should review the duties and access capabilities of staff and implement, to the extent practicable, a proper separation of duties.

Finding No. 2:
Disaster Recovery Plan and Process

IT disaster recovery plans 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. Disaster recovery planning identifies and provides information on supporting resources needed and the roles and responsibilities of those involved in the recovery process. Additionally, testing the plan is essential to determine whether the plan functions as intended in an emergency situation, with the most useful tests simulating a disaster to test the overall service continuity.

During our audit, we continued to note certain deficiencies related to the disaster recovery plan. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising the District's disaster recovery plan. However, appropriate District management have been notified of the deficiencies.

Recommendation: The District should implement, and periodically test, a disaster recovery plan that will enable it to timely resume processing in the event of a disaster.

**Finding No. 3:
Off-Site Backup**

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. One example is routinely backing up data files and programs and securely storing them at an off-site location. Such actions maintain the organization’s ability to restore data files, which may be impossible to recreate if lost.

The District used a tapeless backup system for backing up data files and programs on a nightly basis. The system had a primary backup storage on-site and a mirror copy for off-site storage. The District did not currently store the mirror image off-site, but indicated that it would begin off-site storage during the month of September 2007. District management indicated that it was currently identifying all hardware and network backup needs to ensure that all business requirements are met in case of an emergency.

Failure to remove the mirror image to an off-site location increases the risk that the District may not be able to timely recover all data and programs if a disaster were to occur at the data center facility.

Recommendation: The District should take necessary steps to ensure that backups are stored off-site.

PRIOR AUDIT FINDINGS

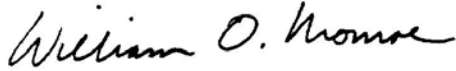
Finding Nos. 1 and 2, noted above, included issues repeated from audit report No. 2005-109 and from the predecessor auditor’s management letter dated October 20, 2006. Other prior IT-related deficiencies, which were within the scope of this audit, have either been corrected or were in the process of being corrected.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected District IT controls and to determine whether the District had corrected, or was in the process of correcting, IT-related deficiencies disclosed in audit report No. 2005-109 and by the predecessor auditor in its management letter dated October 20, 2006. Our scope focused on evaluating selected IT controls applicable to the SAP financials application during the period July 2006 through June 2007. 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, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated August 31, 2007, the District's General Counsel 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 Hjoningram@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.myflorida.com/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.

APPENDIX A
MANAGEMENT RESPONSE



Orange County Public Schools

445 West Amelia Street Orlando, FL 32801-1129 Phone 407.317.3200 www.ocps.net

August 31, 2007

William O. Monroe
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Re: District Response: Information Technology Audit of the Orange County School Board

Dear Mr. Monroe,

Enclosed is the Information Technology Audit of the Orange County School Board, Orange County Public Schools Response.

If you have any questions, please do not hesitate to call me.

Sincerely,

A handwritten signature in black ink that reads "Frank Kruppenbacher". The signature is written in a cursive style with a large, prominent 'F'.

Frank Kruppenbacher
General Counsel

"The Orange County School Board is an equal opportunity agency."

**AUDITOR GENERAL
 INFORMATION TECHNOLOGY AUDIT OF THE ORANGE COUNTY SCHOOL BOARD
 ORANGE COUNTY PUBLIC SCHOOLS RESPONSE**

Finding No. 1 – Security Management

The district is currently moving forward on several fronts to answer some of the issues that were raised with the security audit. We are currently in the middle of a project that will help us transition from our operating system. During this project, we will be able to address the specific issues brought out in the audit. ICTS has also asked for a second security administrator that will address our need to monitor security incidents and assist in the development and maintenance of policies and procedures. These findings will be reviewed as a standard agenda item for the Security Review Team to ensure that our responses are implemented.

RESPONSE TO EACH INDIVIDUAL FINDING COMPONENT

1. The district will collect best practices and develop a process for a quarterly review of assigned security. This plan will be developed for implementation during the 2007 calendar year under the direction of the Chief Operating Officer. The district currently has one Information Security officer. ICTS has requested a second position to deal with the review of access rights, violations and the update of written policies and procedures.
2. The district is in the process of migrating to a new operating system. The findings listed will be nullified by this project. Findings have been noted and corresponding items in the new operating system will be addressed. These have been incorporated into the project plan. ICTS is committed to resolving all outstanding issues within the 2008 fiscal year.
3. The district ICTS department will ensure that the documentation will be updated by December 2007.
4. The district currently has one Information Security officer. ICTS has requested a second position to deal with the review of access rights, violations and the update of written policies and procedures.
5. The district will document those identified having improper access and work with the business areas to remedy any situation where incompatible duties are verified. The same will be done with ICTS staff and implemented where the district feels it is prudent.

Finding No. 2 – Disaster Recovery Plan and Process

The district realizes the importance of a comprehensive Disaster Recovery Plan and Process. To address the issues that the district recognized prior to the audit, external expertise in this area was engaged to assist ICTS in developing a comprehensive plan that would be incorporated into the district Business Continuity Plan. This is an active project and progress is being made. Some of the points that will be addressed by the project are:

1. Identification and documentation of business critical systems
2. Proper backup and recovery procedures for the identified systems
3. Alternate data center hot site with proper equipment
4. Policies and procedures on the periodic testing of the various systems
5. Procedures for the activation of the alternate data center and staffing

Finding No. 3 – Off Site Backup

The district realizes the importance of safeguarding the backups of critical systems in a safe off-site environment. All the equipment has been installed and the mirror image hardware will be moved to another OCPS location until a permanent site is chosen. This will ensure that our backups are safely stored.

THIS PAGE INTENTIONALLY LEFT BLANK