



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



DUVAL COUNTY

DISTRICT SCHOOL BOARD

Information Technology Audit

SUMMARY

The Duval County District School Board (District) maintains SAP enterprise resource planning (ERP) software that provides application processing for the District administrative systems, such as general ledger, accounts payable, human resources and payroll functions. Our audit focused on evaluating selected information technology (IT) functions and determining the effectiveness of selected controls applicable to the District for the period October 2004 through January 2005, evaluating selected SAP activity logging configurations, and determining the status of selected prior audit deficiencies.

As described below, we noted deficiencies in certain general controls related to the District's functions and practices:

Finding No. 1: The District had inadequate segregation of duties that permitted staff that develop applications to also have access to update production application data. In addition, the General Director of the Applications Department also had unnecessary physical access to production computer equipment.

Finding No. 2: A fire extinguisher located in the District's server room had not been inspected in over a year.

Finding No. 3: The District had not maintained a current disaster recovery plan.

Finding No. 4: Not all back-up tapes for the SAP System were properly located at the off-site vault. Additionally, one back-up tape was not properly secured and two tapes were missing.

Finding No. 5: Deficiencies were noted in the District's IT security controls.

BACKGROUND

SAP ERP software was operated in a client-server environment under management of the Division of Technology within the District. The Division of Technology was responsible for providing IT resources to meet the needs of the District. The Applications; Operations; Release Management; and Project Management, Training, Security, and Infrastructure Departments were the functional areas that reported to the Chief Information Officer, Division of Technology.

Finding No. 1:
Segregation of Duties

Segregation of work responsibilities is fundamental, so that one individual does not control all critical stages of a process. In the IT environment, a proper segregation of duties would include a separation of the programming function from the user and operations functions. In addition, activities that cannot be segregated and are inherently risky should be subject to relatively extensive monitoring.

Staff within the Applications Department were responsible for SAP application development, maintenance, functional support, configuration, enhancements, and reports. However, several Applications Department staff, including contractors, could perform both programming and user functions, in that they could create program code for SAP enhancements while also having extensive access to update data from within the SAP application. According to District staff, the ability to update SAP application data was granted to allow the Applications Department to provide support during the July 2004 SAP upgrade, as well as to support SAP application users. While the District maintained and reviewed some logs of changes to data made through the SAP application, procedures had not been implemented to specifically monitor the activities of the aforementioned Applications Department staff. As a result of our audit

inquiries, the District has reduced the access of one contractor.

Our audit further disclosed that the General Director of the Applications Department had access to the computer room where the SAP computer servers reside. This access did not appear to be required as a part of the General Director's responsibilities.

Without an adequate segregation of duties or extensive monitoring, the risk is increased that one person could subvert normal controls resulting in unauthorized changes to programs and data and that computer resources could be damaged or destroyed.

Recommendation: To the extent practicable, the District should separate incompatible functions by prohibiting application development and maintenance staff from also being able to update data. In those instances in which such duties cannot be segregated, the District should implement procedures to monitor these activities. In addition, the District should grant access to computer operation facilities only to those individuals who require the access to accomplish their job responsibilities.

Finding No. 2:
Fire Safety Equipment Inspections

Florida law¹ provides that fire safety equipment should be inspected, serviced, and maintained in accordance with the manufacturer's maintenance procedures and with the applicable National Fire Protection Association standards.

¹ Section 633.065, Florida Statutes

A centralized fire suppression system was in place to protect the District's entire server room, and one hand-held fire extinguisher was available within the server room for localized incidents. Our audit disclosed that the hand-held fire extinguisher had not been serviced for more than six months beyond the annual maintenance requirement as indicated by the attached inspection ticket.

Absent timely inspections of fire suppression equipment in accordance with the Florida law, the risk is increased that inoperable equipment will not be detected and the safety of the District's IT staff and equipment will be jeopardized.

Recommendation: The District should ensure that all fire safety equipment is inspected in a timely manner consistent with Florida law.

**Finding No. 3:
Disaster Recovery Plan**

Disaster recovery 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. Disaster recovery planning identifies and provides information on supporting resources needed and the roles and responsibilities of those involved in the recovery process.

While the District had a disaster recovery plan, the plan had not been updated in over three years. The lack of a current disaster recovery plan could hinder the effectiveness

of District efforts to provide continuous service to meet business requirements in the event of a major disruption.

Recommendation: The District should update its disaster recovery plan and distribute it to applicable staff.

**Finding No. 4:
Back-up Tape Procedures**

Sound backup and retention procedures for IT-related media include provisions for the secure storage, both on-site and off-site, of backed-up data files, software, and related documentation. It is important that accurate records be maintained of the location of backups and that storage sites are periodically inspected for adequate physical security measures.

During our testing of the location of the SAP back-up tapes, we noted several discrepancies between the catalog list of tapes that should have been in the off-site vault and the actual location of the tapes. Eleven of the 21 tapes tested were not appropriately located at the off-site vault. Eight were located inside the computer room, one was located at an employee's residence, and two were not located. With the exception of the tape located at the employee's residence and the two un-located tapes, all tapes were physically secure.

The risk exists that sensitive data could be disclosed as a result of unsecured or missing back-up tapes. Additionally, the District's ability to timely and accurately recover its SAP processing, should a failure in processing

occur, may be jeopardized by deficient tape inventory practices.

Recommendation: The District should take necessary steps to ensure that all tapes are properly accounted for and that the back-up tapes are properly rotated off-site.

**Finding No. 5:
Security Controls**

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. 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 security control features to enhance the security over the District's data and programs.

PRIOR AUDIT FINDINGS

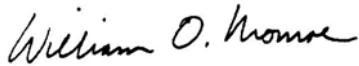
The District had corrected, or was in the process of correcting, portions of IT-related deficiencies noted in audit report No. 02-190 that were within the scope of our audit. One issue within Finding No. 5 was previously noted in audit report No. 02-190 and remained unresolved.

OBJECTIVES, SCOPE, AND METHODOLOGY

The scope of this audit focused on IT controls applicable to the Duval County District School Board during the period October 2004 through January 2005. Our objectives were to determine the effectiveness of selected controls related to the District, to evaluate selected SAP activity logging configurations, and to determine whether the District had corrected, or was in the process of correcting, selected deficiencies disclosed in audit report No. 02-190. 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

DISTRICT'S RESPONSE

In a letter dated March 23, 2005, 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 Art Wahl, CPA*, CISA, and supervised by Tina Greene, 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.

DUVAL COUNTY PUBLIC SCHOOLS

John C. Fryer, Jr.
Superintendent

AIM HIGH

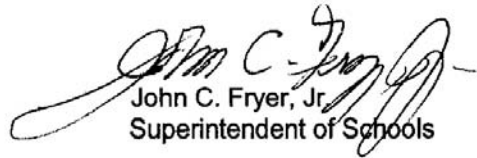
March 23, 2005

Mr. William Monroe, CPA
Auditor General
G74 Claude Pepper Bldg
111 West Madison St
Tallahassee, FL 32399-1450

Dear Mr. Monroe,

Please find the attached response to your 2004 IT audit of Duval County Public Schools. Our district's contact person for questions regarding the audit is Craig Honour, CIO, Information Technology Division (904) 390-2525.

Sincerely,



John C. Fryer, Jr.
Superintendent of Schools

JCF: beh

Attachment: 1

1701 Prudential Drive Jacksonville, Florida 32207-8182
World Wide Web: <http://www.educationcentral.org>

Phone: (904) 390-2115
Fax: (904) 390-2586

March 23, 2005

State Auditors General Findings for the 2004 IT Audit of Duval County Public Schools

Finding 1:

The District had inadequate segregation of duties that permitted staff that develop applications to also have access to update production application data. In addition, the General Director of the Applications Department also had unnecessary physical access to production computer equipment.

District Response:

DCPS concurs with the importance of segregation of duties and auditor finding that a developer had access to both development and production environments and the General Director for Applications had unescorted physical access to SAP servers. General Director was on list for physical access to the SAP server room as a result of reorganization but access was never exercised. The access was removed. The SAP production servers were moved to a new data facility in March 2005 and access to the new facility is now restricted to operations and security staff (13 total). Developer access to production is more problematic as the developers have also filled Analyst and Operator roles. DCPS has several essential custom programs that require developer access to production system to run. DCPS will identify those essential transactions that we need developers to run and either reassign them to operators or modify them so that they can be reassigned to operators. Upon completion we will remove developer access to production to restore segregation. In the interim to mitigate risk, DCPS will create audit trace of developer actions and analyze the trace monthly.

Finding 2:

A fire extinguisher located in the District's server room had not been inspected in over a year.

District Response:

DCPS concurs that the fire extinguisher was out of date. It has since been inspected and certified as operational. Throughout the period of time that the secondary fire extinguisher was out of date, the server room was protected by the built in primary inert gas fire extinguishing system.

1

Finding 3:

The District had not maintained a current disaster recovery plan.

District Response:

DCPS concurs that the District IT disaster recovery plan needs updating. DCPS is assessing 2004 hurricane lessons learned from harder hit counties and disaster recovery issues relating to new data center. The plan is scheduled for update by June 2005.

Finding 4:

Not all back-up tapes for the SAP System were properly located at the off-site vault. Additionally, one back-up tape was not properly secured and two tapes were missing.

District Response:

DCPS concurs that not all backup tapes were at off-site vault, one tape was not properly secured and two tapes were missing. The inspection immediately followed an actual hurricane. Tapes were dispersed for hurricane but not retrieved. All tapes are now properly accounted for. DCPS moved production SAP servers to new data center and has outsourced off-site SAP back-up tape management as part of the new data center contract. Internal controls on back-up tapes for lesser SAP test, QA, and sandbox systems have also been tightened.

Finding 5:

Deficiencies were noted in the District's IT security controls.

District Response:

DCPS concurs that there were minor deficiencies in IT security controls. Although the deficiencies offered opportunity for security breach, no security breaches occurred and the deficiencies have been corrected.