



# AUDITOR GENERAL

WILLIAM O. MONROE, CPA



## LEON COUNTY DISTRICT SCHOOL BOARD TOTAL EDUCATIONAL RESOURCE MANAGEMENT SYSTEM Information Technology Audit

### SUMMARY

The Leon County District School Board (District) utilizes the Total Educational Resource Management System (TERMS) to provide application processing for personnel, payroll, and finance-related functions. TERMS software processes financial data that supports functions such as vendor management, budget, purchasing, warehouse requisitions, and general ledger.

Our audit focused on evaluating selected information technology (IT) controls applicable to the TERMS Financial Information System during the period September 2005 through January 2006, and determining the status of corrective actions regarding selected prior audit findings disclosed in audit report No. 03-197.

The results of our audit are summarized below:

**Finding No. 1:** TERMS application security activity, such as modifications to user access privileges, was not systematically logged by the District, limiting the ability to monitor the appropriateness of security administration actions.

**Finding No. 2:** Improvements were needed in the segregation of duties within the Technology and Information Services area with regard to the ability of programming staff to modify and execute programs against production data without detection.

**Finding No. 3:** The District did not have adequate written policies and operating procedures for TERMS users within the Finance Department.

**Finding No. 4:** Deficiencies were noted in network security controls in the District.

**Finding No. 5:** District procedures for the removal of network access privileges of terminated employees needed strengthening.

**Finding No. 6:** Improvements were needed in the District's storage and control of back-up tapes.

**Finding No. 7:** Improvements were needed in District procedures for the disposal of IT equipment.

### BACKGROUND

The District purchased TERMS from Educational Data Resources, Inc. (EDR) in 1982, and implemented the software in 1983. The system is written in COBOL and the on-line component runs under Customer Information Control System (CICS) on an International Business Machine (IBM) mainframe running the OS390 Multiple Virtual Storage (MVS) operating system. Data is collected and updated on-line as well as with batch jobs. Reporting is also requested on-line and through submitted batch jobs. The TERMS application is used for personnel, payroll, and finance-related functions. The user community is composed of administrative staff

from all Leon County School Board departments, including schools. Users have two options for connecting to the mainframe; TN3270 terminal emulation software or Web-based access through the District's web portal. In addition, a TERMS Web Job Submission System has been developed which enables users to submit batch jobs for TERMS from the web.

Over the years, customizations have been made to the original system by the District's Technology and Information Services (T&IS) staff. Maintenance and support for the TERMS application is provided in-house by T&IS staff. As of the completion of our audit field work, there was no new development activity underway relating to the TERMS application. The District planned to replace the existing mainframe TERMS application with a two tier client-server environment and was in the process of obtaining funding for the TERMS replacement.

While T&IS is primarily responsible for IT support, technical support is also provided by IT technology contacts who are individuals selected by a District principal or administrator to function as a liaison between the school site or departmental office they represent and the District's Technology and Information Services Division. Technology contacts are also responsible, at many sites, for configuring and maintaining local area networks and servicing the needs of users, including on-site training.

---

#### **Finding No. 1:**

##### **Logging of Security Activity**

---

Good IT security practices include maintaining an automated log of security administration activity to determine how, when, and by whom specific actions were taken. Security logs provide the

ability to, among other things, selectively identify access modifications made by security personnel.

The TERMS package included security functionality to monitor and control the TERMS application users' access. TERMS application security was administered through the TERMS - General Support Series, Security Record function. However, the General Support Series did not maintain an automated log of access modifications made by security personnel.

Without logs of activity within the security administration function, the District may be unable to determine when or by whom a user's access was modified or deleted. The lack of logging the application security activity could hinder the District's ability to pinpoint accountability for a breach of security, should it occur.

---

**Recommendation: The District should implement a logging feature within the General Support Series, Security Record function to capture modifications made to users' application access privileges. However, if this is not deemed cost effective due to the time frame for the system's anticipated replacement, the District should ensure that the replacement system generates and maintains logs of access modifications made by security personnel.**

---

#### **Finding No. 2:**

##### **Segregation of Duties**

---

Segregation of incompatible duties is an important element of internal control. An appropriate division of roles and responsibilities can assist in the detection of errors or fraud and exclude the possibility for a single individual to subvert a critical process. In the IT environment, good business practice suggests that segregation of duties be in place with regard to program changes, the movement of programs into the

production environment, and the updating of production data. If segregation of duties is difficult to accomplish because of a limited number of personnel, compensating controls, such as close monitoring of the modification and execution of programs, may be necessary.

The District's practice was for programmers within T&IS to modify the programs and then move them into the production environment. As noted in audit report No. 03-197, the District implemented a compensating control that was intended to ensure that the programmer could not move changed code into the production environment without detection. Program move activities were being monitored by appropriate staff through automated e-mail notifications and review of program move history files.

However, our audit testing determined that the programmers could run modified programs, with update capability against production data, from either the test or production libraries without any logging or review of activity in the test library. Consequently, unauthorized code could be processed against production data directly from the test library without the need to first move the program into the production library. As a result, District monitoring of program move activity could be circumvented and unauthorized changes to data could go undetected.

---

**Recommendation: The District should review T&IS' access privileges and more appropriately restrict staff's system access to the IT resources for which they are responsible.**

---



---

**Finding No. 3:**  
**User Operating Procedures**

---

Written policies and procedures help ensure that personnel understand their roles and responsibilities and that management directives

are correctly and consistently applied. TERMS users included staff within the Finance Department.

Our audit disclosed that comprehensive written policies and procedures were not in place to guide Finance Department activities. At the end of our audit field work, a Finance Department Procedural Guide was under development but had not been distributed to the Finance Department staff. Additionally, certain individuals within the Finance Department had developed their own informal desk procedures or instructions for some of their specific job functions and duties; however, these procedures were not centrally or formally maintained.

In response to our inquiries, the District anticipated that the Finance Department Procedural Guide would be completed and distributed by April 1, 2006. In the absence of comprehensive written policies and procedures, the risk exists that Finance Department staff will not carry out their responsibilities in accordance with management's intent or in a consistent manner.

---

**Recommendation: The District should implement a plan to ensure that written policies and procedures are completed, approved, and distributed to Finance Department staff.**

---



---

**Finding No. 4:**  
**Network Security Controls**

---

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Effective security practices include the restriction of logical access to and use of IT computing resources through the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Such

mechanisms help to prevent unauthorized individuals from accessing computer resources.

Our audit disclosed the following:

- The District had not installed a network intrusion detection or prevention system. While the District had previously attempted, during December 2004, to purchase an intrusion detection or prevention system, through a formal Request for Proposal (RFP) process, the process did not result in a purchasing decision. Subsequent to our field work, the District issued a second RFP for this type of product. The proposals were due January 18, 2006, and as of the end of our field work, a final decision regarding the purchase had not been made.
- The District's default domain policy allowed the network to maintain a list of the last five passwords used by a network user. However, the minimum password age for network passwords was set to zero days, which would allow users to immediately "cycle through" a set of passwords in order to return to their original password. In response to our inquiries, the District indicated that the minimum password age setting was strengthened, effective December 8, 2005.
- The District required network users to provide specified information to verify their identity when the user requested an immediate resetting of their password. However, the District had not prepared written procedures reflecting this practice. In response to our inquiries, the District indicated that Section O.60.005G of the Operation Techniques Manual was modified on December 8, 2005, to include the requirement that specified information be provided to verify user identities prior to resetting their passwords.

- We noted additional deficiencies in certain District network security controls in the areas of monitoring network security, authentication of users, and control of wireless access points. Specific details of these deficiencies are not disclosed in the report to avoid the possibility of compromising District information. However, appropriate personnel have been notified of these deficiencies.

Without effective network security controls to detect or restrict access to and use of IT computing resources, the District's risk is increased of not preventing or detecting unauthorized personnel gaining access to, modifying, or destroying network available resources and data.

---



---

**Recommendation:** To reduce the risk of unauthorized personnel gaining access to, modifying, or destroying network available resources and data, the District should strengthen its network security controls by implementing an intrusion detection or prevention system and addressing the additional deficiencies noted above.

---



---

#### **Finding No. 5:**

#### **Management of Access Privileges**

Effective security practices include periodic reviews of user access rights. Comparisons of resources with recorded accountability reduce the risk of errors, fraud, misuse, or unauthorized alteration.

Our audit disclosed the following:

- It was District practice to allow school technology contacts to perform an informal review of access revocations of terminated employees. T&IS staff, on an annual basis, also performed a review of access revocations. However, the District did not have written procedures that outlined the steps necessary for the periodic review of network access

privileges to ensure that terminated employee's access was removed timely. In response to our inquiries, the District indicated that, as of December 2005, an access review or confirmation process was established which applied to enterprisewide mainframe and network-based student and business systems. The District further indicated that review of terminations would occur consistent with the official School Board approved record of position terminations, on no less than a monthly basis.

- Twenty-one employees who had terminated employment with the District did not have their network access deleted in a timely manner. Network access, for these individuals, remained active between 14 and 210 days after their dates of termination. In response to our inquiries, the District indicated that school administrators and technology specialists would be reminded to make timely requests for access removals and be required to review employees shown as terminated, via a monthly listing from Personnel, to confirm the deletion of network access.
- As of the completion of our audit testing on October 4, 2005, an additional 40 employees had retained network access privileges for periods ranging from 34 to 256 days after their dates of termination. In response to our inquiries, the District indicated that the access privileges for 12 of these individuals were disabled or deleted by December 9, 2005, and that the balance of the access privileges were subsequently disabled or deleted.

Allowing unnecessary or inappropriate access capabilities to remain active for terminated employees increases the risk of unauthorized disclosure, modification, or loss of data and IT resources.

**Recommendation: The District should strengthen its controls related to the removal of unneeded access privileges in order to minimize the risk of compromising the District's data and information resources. Specifically, the District should enhance its procedures to ensure the immediate removal of terminated employees' access and the timely performance of periodic access reviews.**

#### **Finding No. 6:**

#### **Tape Back Up Procedures**

IT resource controls dictate that back-up procedures be implemented to ensure the proper storage of IT-related media containing data files, software, and related documentation, both on-site and off-site. IT resource controls also ensure that back-up media is stored securely with storage sites periodically reviewed for physical access security.

Our audit disclosed the following:

- On special occasions, such as the end of the calendar year, certain IT staff would take the official back-up tapes to their residences because the normal storage location may not have provided access to the tapes in a timely manner. In addition, the Operation Techniques Manual, Section No. O.70.013D provided that certain IT staff could store District back-up tapes in their residences. The storage of tapes in a personal residence increases the risk that the tapes may be lost, damaged, or not available to the District in a timely manner. In response to our inquiries, the District indicated that, effective December 5, 2005, procedures were modified to provide that a designated individual, with vault access and supervisory responsibility, would be available for the placement of tapes in the District's fireproof vault.
- The District stored off-site back-up tapes in a facility which was geographically close to its IT operations center. At the time of

our audit, the District was in the process of locating another storage site that was not geographically close to the IT operations center to mitigate the risk of a wide area natural disaster destroying both the IT operations center and off-site back-up tape locations. In response to our inquiries, the District indicated that specific operational details will be considered for out-of-state and off-site backup storage sites and finalized by June 30, 2006.

Inadequate storage and control of back-up tapes may lead to the inadvertent physical damage or loss of tapes.

---

**Recommendation: The District should continue with its enhancements to the off-site backup processes and update related procedures accordingly.**

---

#### Finding No. 7:

#### IT Equipment Disposal

IT resource controls dictate that procedures be implemented to prevent access to sensitive information and software on computers, disks, and other equipment or media when these items are disposed of or transferred to another use. Such procedures ensure that data deleted from equipment to be disposed cannot be retrieved by any internal or third party. IT resource controls also include the logging of disposed sensitive items to maintain an audit trail.

Our audit disclosed the following:

- T&IS procedures for erasing Apple and Windows system hard drives did not include the requirements that computers were to be logged as erased prior to leaving the facility. In response to our inquiries, the District indicated that, on November 8, 2005, its Transfer of Property Form was modified to require a certification by the site administrator that hard drives have been cleansed.

- Prior to September 21, 2005, the District's practice was for Purchasing (warehouse) staff to use a Transfer of Property form to record information about surplus IT equipment. Such information included sale number, cost, property control number, description, and whether or not the item was junked or recycled. However, the warehouse staff did not use the above form, or have policies and procedures in place, to log when computer hard drives were erased and by whom. Subsequent to our inquiries, an additional Computer Equipment Final Disposition Log was implemented that indicated the method of hard drive disposal used, the date of the disposal, and the name of the individual who erased or destroyed the hard drive. Also, in response to our inquiries, the District indicated that warehouse staff were retrained the week of November 8, 2005, and that written procedures for warehouse staff were put in place November 16, 2005.

- We noted additional aspects of the District's procedures for the disposal of IT equipment that needed improvement. Specific details of these deficiencies are not disclosed in the report to avoid the possibility of compromising District information. However, appropriate personnel have been notified of these deficiencies.

Absent effective practices and written procedures governing the process of sanitizing and releasing surplus IT equipment, including documentation requirements, the risk is increased that such activities will not be consistently performed and that confidential and sensitive information may be released to unauthorized individuals.

---

**Recommendation: The District should continue with its enhancements to the surplus computer disposal processes and update related procedures accordingly to reduce the possibility of improper disclosure.**

---

---

---

**PRIOR AUDIT FINDINGS**

---

---

Findings No. 2 and 6, noted above, included issues repeated from our prior audit report No. 03-197. Other IT deficiencies noted in the prior audit, that were within the scope of this audit, have been corrected or were in the process of being corrected.

---

---

**OBJECTIVES, SCOPE, AND METHODOLOGY**

---

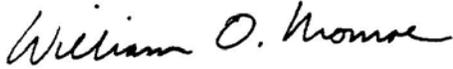
---

The objectives of this audit were to determine the effectiveness of selected general and application IT controls of the District. Our audit scope focused on selected IT controls applicable to the TERMS Financial Information System during the period September 2005 through January 2006. We also determined whether management had corrected, or was in the process of correcting, selected IT-related deficiencies disclosed in audit report No. 03-197.

In conducting this audit, we interviewed appropriate District personnel, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to TERMS.

**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 April 6, 2006, 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 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 Earl Butler, CISA, and supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA\*, CISA, Audit Manager, via e-mail at [joningram@aud.state.fl.us](mailto: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.

APPENDIX A  
MANAGEMENT RESPONSE

BOARD CHAIRMAN  
H. Fred Varn

BOARD VICE-CHAIR  
Maggie B. Lewis



BOARD MEMBERS  
Georgia "Joy" Bowen  
Sheila Costigan  
Dee Crumpler

SUPERINTENDENT  
William J. Montford, III

April 6, 2006

Mr. William O. Monroe, CPA  
Auditor General  
P.O. Box 1735  
111 West Madison Street  
Tallahassee, FL 32302

Dear Mr. Monroe:

Enclosed is the written response regarding the tentative findings reflected in the Preliminary Audit Report for Information Technology of the Total Educational Resource Management System (TERMS) for Leon County District School Board for the period September 2005 through January 2006.

We would like to thank you for this opportunity to respond to audit findings as this will enable us to address issues which will facilitate the District's ability to provide better services to students. Should you need any further clarification or information, please feel free to contact us.

Sincerely,

Handwritten signature of William J. Montford, III in cursive script.  
William J. Montford, III  
Superintendent

Attachment

Cc: All School Board Members  
School Board Attorney  
Assistant Superintendents  
Internal Auditing

Mr. William O. Monroe, CPA  
 April 6, 2006 (REVISED)  
 Page 2 of 3

**Finding No. 1:  
 Logging of Security Activity**

**Response to Finding No. 1:** Automatic Logging of Access to the TERMS General Support Series - One of the TERMS Finance system modules, the General Support Series, does not implement an automatic logging function. There is currently in place a manual procedure, which requires a signed and dated authorization request form be submitted and kept on file for any access change. Update access in this series is restricted to a very small number of people in the Finance and Payroll departments.

The replacement ERP system specifications will include the capability to also automatically generate and maintain logs of access modifications made. Pending approval of the requested funding, the process of replacing TERMS is expected to begin in fall, 2006.

**Finding No. 2:  
 Segregation of Duties**

**Response to Finding No. 2:** Segregation of Duties – recommending further restriction of selected Applications staff being able to initiate updates of TERMS production data, without logging or review of activity. Currently, all programs compiled in production, including programs which update production data, are automatically logged. A planned migration away from the mainframe environment is already in progress which minimizes instances of running modified programs in test mode. While this shift is in progress, monitoring efforts will be strengthened. Thus, minimal application development in

the current mainframe environment is planned since these systems are scheduled for replacement by fall, 2008. All future enterprise systems (student and business) will become distributed client-server based solutions. With this transition comes a commitment to a life cycle management model as defined by distinct – and functionally separate - R&D, Quality Assurance, and Production/Operation phases. Specific controls will include source code management and database logging (such as are available through SQL logging and Lumigent) of all enterprise database activity. Consistent with this plan, there are already established separations of database, applications development, and production functions in the recent roll-out of the converted student enterprise application (Genesis). This separation of duties will also occur in the conversion to the new ERP system.

**Finding No. 3:  
 User Operating Procedures**

**Response to Finding No. 3:** The Finance Department has submitted a plan and schedule for updating and providing written policies and procedures as recommended. The written procedures are being updated and should be ready for distribution by the first week in April 2006.

Mr. William O. Monroe, CPA  
April 6, 2006 (REVISED)  
Page 3 of 3

**Finding No. 4:  
Network Security Controls**

**Response to Finding No. 4: Network Security Controls** – The purchase of an automated intrusion detection system had already been planned and is scheduled to be purchased in fiscal year 2007-08. Purchase in this timeframe enables the school district a discount of approximately 58% via the federal E-rate program. There have been no significant pattern of network service disruptions over the past three years (99%+ uptime), and this delay is considered reasonable. The other network security issues identified (relating to increasing the minimum password age, verification of user identity when password requests are made, and wireless access) had already been addressed and documented.

**Finding No. 5:  
Management of Access Privileges**

**Response to Finding No. 5: Removal of Terminated Employees Access Privileges** Currently, the respective supervisor of a terminated employee is responsible for notifying the site technical specialist or the district Help Desk so that access authorizations are disabled in timely order. These procedures are in writing, are a regular part of the security training and review provided to district school and cost center administrators; and are listed on the employee termination checklists. With the emphasis on the importance of these steps to

administrators, and the confirmation of terminated employees access following official School Board action on those employees, timely action should be more consistent. (Note: automated disabling of user network access, immediately based upon termination approval, will also be a requested feature in the replacement ERP system).

**Finding No. 6:  
Tape Back Up Procedures**

**Response to Finding No. 6: Tape Back-up Procedures** had already been changed to permit tape back-ups to be placed during the holiday break period in the fireproof vault. Offsite back-up is currently provided for highly critical systems at Northwest Regional Data Center. Also, options for having more geographically remote back-ups have been under evaluation and are expected to be completed by fall, 2006.

**Finding No. 7:  
IT Equipment Disposal**

**Response to Finding No. 7** Cleansing of Salvaged or Surplus Electronic Equipment Procedures for confirming that salvaged or surplus electronic equipment is properly disposed were already introduced this past year and have been reviewed to ensure all steps necessary for compliance with the auditors' recommendations are in place.

**THIS PAGE INTENTIONALLY LEFT BLANK**