



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



LAKE COUNTY DISTRICT SCHOOL BOARD

TOTAL EDUCATIONAL RESOURCE MANAGEMENT SYSTEM

Information Technology Audit

SUMMARY

The Lake County District School Board (District) utilizes the Total Educational Resource Management System (TERMS) to manage its financial resources. The eight components of the TERMS Financial Information Series provide functionality that support activities ranging from initial budget preparation through year-end reporting. The components are used by school and department personnel, as well as District-level staff and District board members.

Our audit focused on evaluating selected information technology (IT) controls applicable to the TERMS Financial Information Series during the period September 2005 through February 2006, and determining the status of corrective actions regarding selected prior audit findings disclosed in audit report No. 03-185.

The results of our audit are summarized as follows:

Finding No. 1: District procedures for authorization of access to the network and TERMS were not followed in all instances.

Finding No. 2: TERMS Financial Information Series emergency and temporary access requests were not approved by either the Chief Financial Officer or the Finance Director, the functional owners of the TERMS Financial Information Series data. Instead, they were approved by the Information Services Manager.

Finding No. 3: Access capabilities to TERMS had been granted to users who did not need the access for their job function. Additionally, access to sensitive functions within the AS/400 mid-range computer environment was not appropriately limited.

Finding No. 4: 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. 5: We noted instances where the District did not remove access privileges for terminated employees in a timely manner.

Finding No. 6: Improvements were needed in certain security controls protecting TERMS.

Finding No. 7: The TERMS change management process needed strengthening.

Finding No. 8: We noted instances where the District's IT Standard Operating Procedures needed enhancement.

Finding No. 9: The District had in excess of 4,000 IT surplus personal computers (PCs) in storage. The hard drives of those PCs had not been prepared for disposal and were stored in facilities that were not environmentally controlled.

Finding No. 10: Out-of-lease student PCs were not approved for disposition prior to being prepared and sold to students.

Finding No. 11: Certain other District procedures related to the disposition of IT surplus equipment were not effective.

Finding No. 12: Certain deficiencies related to the IT disaster recovery plan continued to exist.

Finding No. 13: Procedures for the storage of AS/400 back-up tapes at designated off-site facilities were not followed.

Finding No. 14: Physical security controls over the District's IT facilities continued to need improvement.

BACKGROUND

Pursuant to Florida law¹, each district school board is responsible for maintaining accurate records of all financial transactions. To provide for this and other required functions, the District used TERMS. The TERMS Financial Information Series V3R1 is composed of eight components, including, in part, budgeting, purchasing, accounts payable, accounts receivable, and general ledger. These components run on an IBM iSeries (AS/400) mid-range computer utilizing an OS/400 operating system. TERMS users are connected to the application by the District's wide area network.

The District serves a population of approximately 38,000 students and 4,700 faculty and staff. Students, faculty, and staff rely on the IT infrastructure and services to accomplish their assigned tasks. As a result of this reliance, IT services are considered a critical component to the daily operations of the District. The IT Department is under the direction of the District's Chief Technology Officer. The IT Department has two primary components, Information Services (IS) and Technology. The Information Services Manager oversees application development and the AS/400. The Technology Manager manages the technology infrastructure and personal computer support.

**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 transferred to security managers. The District's IT Standard Operating Procedures state that District employees needing network access must complete a *LCSB Network User Account Registration* form. The applicant's principal or supervisor signs the form and forwards it to the IT Department. Employees needing access to the Financial Information Series of TERMS must complete the *IS Security* page on the District's IS

Web page and submit it to IS. Either the Chief Financial Officer or Finance Director must approve the access privileges.

During our audit, we requested evidence to support 16 new employees' user access privileges to the network and the Financial Information Series of TERMS. We noted the following:

- Four of the 15 new employees tested who had access to the District's network did not have documentation to support supervisory authorization for their access capabilities.
- Three of the nine new employees tested who had access to the TERMS Financial Information Series did not have documentation to support supervisory authorization for their access capabilities.

Failure to document access authorizations increases the risk of inappropriate access and unauthorized use, disclosure, or modification of data and programs.

Recommendation: The District should ensure that the access control procedures detailed in the IT Standard Operating Procedures are followed.

**Finding No. 2:
Emergency and Temporary Access**

Good IT security practices dictate that emergency and temporary access authorizations be documented on standard forms and maintained on file, approved by the functional owner, securely communicated to the security function, and automatically terminated after a predetermined period of time. The concept of ownership plays an important role in the determination of responsibility for a specific system's security. The data or functional owner is typically responsible for the approval of authorized users and relevant access privileges.

Our audit disclosed situations when temporary access was required, including, for example, auditor access and consultant access. When these situations occurred, the Information Services Manager in the IT Department rather than the functional owner of TERMS Financial Information Series approved the access requests.

¹ Section 1001.42(10)(f), Florida Statutes

Inadequate controls related to emergency and temporary access increase the risk that individuals may have unauthorized, inappropriate access to data and programs.

Recommendation: The District should ensure that the functional owner of TERMS approves all access authorizations.

Finding No. 3:

TERMS and AS/400 Access Capabilities

The objectives of limiting access are to ensure that users have only the access needed to perform their duties; access to very sensitive resources is limited to very few individuals; and, employees are restricted from performing incompatible functions or functions beyond their responsibility. Our audit disclosed the following:

- Five of the 21 IT Department employees tested had inappropriate update access to the production Financial Information Series of TERMS. Subsequent to our audit inquiries, the District made the appropriate adjustments to these users' access privileges.
- One Computer Systems Analyst (a programmer) had AS/400 access to the all objects special authority, which provided access to all system resources, including the capability to move a program change into the production environment. Subsequent to our inquiries, the District implemented two compensating controls. The Human Resources Department began reviewing the Computer Systems Analyst's paycheck to verify there were no changes, and the IS Manager began reviewing reports that provide monitoring of program changes made to the production environment.
- One IS Quality Assurance Analyst was inadvertently granted the AS/400 security administrator special authority, which provided the ability to add and delete users, change passwords, and grant security officer privileges to other users. Subsequent to our inquiries, the District deleted the Analyst's security administrator special authority access.
- Twenty individuals or user IDs had access to the AS/400 production command line. This privilege provided direct access to the

TERMS production database, bypassing the TERMS application security. In addition, at the time of our audit inquiries, the District was not monitoring users with production command line access. Subsequent to our inquiries, the District removed the production command line access from eight of the twenty individuals or user IDs and implemented a process for monitoring the remaining individuals with production command line access.

Access greater than what is needed to perform an individual's job duties, together with insufficient monitoring of access to sensitive functions, increase the risk of unauthorized disclosure, modification, or destruction of data and IT resources.

Recommendation: The District should periodically review user access to TERMS and sensitive functions within the AS/400 environment to ensure that access privileges are appropriate and commensurate with users' job duties. Additionally, the District should consistently monitor the system actions of users with production command line access.

Finding No. 4:

Logging of Security Activity

Good IT security practices include maintaining an automated log of security activity to determine how, when, and by whom specific actions were taken. Security logs provide the capability of selectively identifying unauthorized, unusual, and sensitive access activity, such as attempted unauthorized access and access modifications made by security personnel.

The TERMS package maintains its own security functionality to monitor and control TERMS application users' access. TERMS application security is administered through the TERMS Application Environment, General Administration Function. However, the Application Environment does 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. Also, as a result of no log of access modifications, we were unable to make a determination as to the timeliness of TERMS application access removal for terminated employees.

Subsequent to our audit inquiries, the District began exploring the possibility of utilizing the AS/400’s journaling function to capture specific logs on certain TERMS database tables, such as the profile table and the user ID table, as a compensating control. These logs would indicate new, changed, and removed TERMS user IDs.

Recommendation: The District should continue to explore the possibility of utilizing the AS/400 journaling function to capture changes to access modifications. If this is not deemed feasible, the District should explore purchasing and implementing a security software product to strengthen the monitoring of the security administration function.

**Finding No. 5:
Terminated Employee Access**

Good IT security practices dictate that appropriate and timely actions be taken regarding job changes and job terminations so that internal controls and security are not impaired by such occurrences.

Upon our audit request, the District provided us a list of terminated District employees for the period January 1, 2005, through October 4, 2005. We noted the following:

- For the 30 terminated employees tested, 8 had not had their network access appropriately disabled or deleted, even though they had been terminated for periods ranging from 46 to 231 days. Of the 8, further audit testing indicated that one did not have his AS/400 access appropriately deleted. Subsequent to our inquiries, the District disabled the network accounts for these eight individuals on November 15, 2005, as well as the AS/400 account for the one individual.
- One additional terminated employee did not have his AS/400 access appropriately deleted.

Subsequent to our inquiries, the District appropriately deleted the individual’s access on December 5, 2005, 584 days after the date of termination.

- Of the 18 terminated Finance and IT Department employees tested, 1 did not have his TERMS user ID deleted in a timely manner. In response to our audit inquiries, the District indicated that the individual’s TERMS user ID was deleted on October 12, 2005, 75 days after the date of termination.
- At the time of our audit testing, the network security administrator was not receiving notification of terminated or transferred employees. Subsequent to our inquiries, the network security administrator began receiving a report generated from the Human Resource System, which identified terminated and transferred employees, for use in the deletion of user accounts.

Lack of effective coordination between the District’s Human Resources Department and the network security administrator may have contributed to the inconsistency in the removal of access capabilities for terminated employees. Without timely deletion of access of employees who terminate employment with the District, the risk is increased that terminated employees’ access privileges could be used to view or modify data.

Recommendation: The District should implement stronger controls over the removal of access privileges in order to minimize the risk of compromising the District’s data and information.

**Finding No. 6:
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 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.

Finding No. 7:

Change Management Process

Establishing controls over the modification of application programs helps to ensure that only authorized modifications are implemented. This is accomplished by instituting procedures that ensure that all program modifications are properly authorized, tested, and approved. Good system testing practices exclude the use of live data for testing and instead provide for developing a comprehensive set of transactions and data that represent the various activities and conditions that will be encountered during processing. Additionally, proper segregation of duties with regard to program change controls includes provisions for the movement of programs into the production environment being controlled by persons independent of the programmer making the program modifications. When this is not practicable, regular monitoring of programs moved into production should be performed.

Certain aspects of TERMS program modification controls needed strengthening. Specifically, our audit testing of eight modifications to TERMS programs disclosed that:

- Three changes did not have documentation to support that independent testing took place prior to being moved into production.
- One change did not have documentation to support that someone other than the person making the program change moved the modified code into production.
- The District was unable to demonstrate that an independent review of the change management audit log, *Security Audit – Restored Objects*, took place.

Additional audit testing disclosed that IS staff used the TERMS production environment to resolve and replicate finance issues.

Weak controls over the modification of application programs increase the risk that unauthorized programs and program modifications may be implemented in the production environment.

Recommendation: The District should strengthen its program change management controls to provide increased assurance that only authorized programs and program changes are implemented in production. Additionally, the District should strictly limit the testing of programs and program changes to the test environment.

Finding No. 8:

IT Standard Operating Procedures

Each function in the organization needs complete, well-documented, policies and procedures to describe the scope of the function, its activities, and the interrelationships with other departments. The District had developed IT Standard Operating Procedures, which documented the guidelines, rules, requirements, and actions that affect IT services at Lake County Schools.

The IT Standard Operating Procedures identified the activities, resources, and procedures needed to carry out IT activities during normal operations. Our audit disclosed that the IT Standard Operating Procedures needed to be enhanced to include written policies and procedures for the following activities:

- The update and removal of user accounts for access to TERMS.
- Requesting, authorizing, and granting emergency and temporary access to TERMS.
- System software changes to the Windows and OS/400 operating systems.
- The use of AS/400 system utilities and sensitive files and the monitoring thereof.
- The network security administration function, including the resetting of user passwords, removal of access for terminated employees, and monitoring of security events.

- The AS/400 security administration function, including the update and termination of user accounts for access to the AS/400.

The absence of written policies and procedures may have contributed to the issues previously discussed in Finding Nos. 2, 3, and 5. Absent formal policies and procedures, the risk is increased that sound information security controls will not be sufficiently established to prevent the compromise of data confidentiality, integrity, and availability.

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

**Finding No. 9:
Surplus PCs**

Proper controls over the disposal of IT equipment include procedures to prevent access to sensitive information and software from IT surplus property such as PCs, disks, and other equipment or media when they are transferred to another use or for storage prior to final disposition. Such procedures ensure that data deleted from equipment to be disposed cannot be retrieved by any internal or third party. Good physical controls over surplus IT equipment being retained for subsequent internal or external use include using a storage facility with sufficient environmental controls in order to ensure that equipment is adequately protected against fire, dust, power, and excessive heat and humidity.

During our audit, we noted the following:

- The District last disposed of District-owned PCs in August 2003. At the time of our audit field work, the District had in excess of 4,000 surplus PCs in storage awaiting final disposition. District staff indicated that the number of surplus PCs continued to grow because the District School Board members had not been able to come to an agreement for the final disposition, such as sale, reuse, donation, or destruction of the equipment.

- The surplus PC hard drives had not been cleansed or removed in preparation for disposition.
- The warehouse and eight rented semi-trailers used to store the surplus PCs were not environmentally controlled.

Failure to timely dispose of computer equipment that has been declared surplus may limit the potential benefit to be derived from the disposition, especially if intended for sale, re-use, or donation to a third party. Additionally, failure to maintain the surplus inventory in environmentally controlled storage facilities increases the risk of damage to the computer equipment.

Recommendation: The District should establish a process for the final disposition of the IT surplus property inventory. The District should also explore possibilities for the future storage of surplus IT equipment in secure, environmentally controlled storage facilities.

**Finding No. 10:
Approval for Disposition**

The District implemented a process whereby out-of-lease student PCs could be prepared and sold to students. In order to ensure that the out-of-lease PCs were disposed of in an efficient and procedural manner, the District's IT Standard Operating Procedures stated that a *Disposition Form* was to be filled out prior to disposition. This form was to be signed by the applicable principal and the Chief Technology Officer, and approved by the District School Board.

At the end of July 2005, East Ridge High School had 500 student PCs come out-of-lease that were either subsequently sold or planned to be sold to students and their families. Our audit testing determined that East Ridge High School did not process the required *Disposition Form* for these student PCs. Consequently, student PCs were either sold, being offered for sale, or planned to be offered for sale that had not been appropriately approved for disposition.

Failure to follow the District's procedures for disposition of computer equipment increases the risk that equipment will be disposed without having been properly authorized.

Recommendation: The District should properly authorize all IT equipment, including student PCs, for disposition prior to disposal.

**Finding No. 11:
Disposal Procedures**

As previously discussed, effective procedures related to the disposal of IT equipment include measures to prepare the equipment for disposal. During our audit, we determined that certain District procedures related to disposition of IT surplus property, in addition to the matters noted in Finding Nos. 9 and 10, needed improvement. Specific details of these issues are not disclosed in this report to avoid any possibility of compromising District information. However, appropriate District management staff were notified of the issues. Subsequent to our notification, the District implemented additional procedures to strengthen controls in the applicable areas.

Recommendation: The District should monitor its procedures related to the disposition of IT equipment to ensure that all equipment is appropriately prepared for disposal.

**Finding No. 12:
IT Disaster Recovery Plan**

Having an operational and tested IT disaster recovery plan ensures minimum business impact in the event of a major disruption and thus continuous service. During our audit, we continued to note certain deficiencies related to the IT disaster recovery plan. Specific details of these deficiencies are not disclosed in this report to avoid any possibility of compromising the District's IT disaster recovery plan. However, the appropriate District management staff have been notified of the deficiencies.

Recommendation: The District should take appropriate steps to ensure the IT disaster recovery plan includes all necessary provisions and is fully integrated into the District's IT environment.

**Finding No. 13:
Back-up Tapes**

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's IT Standard Operating Procedures detailed three scheduled back-ups to be performed on the AS/400 test and production systems: daily, weekly, and monthly. The IT Standard Operating Procedures also specified where these back-up tapes are to be stored. These locations were corroborated by the District's IT disaster recovery plan. At the time of our initial site visit, the District's practice was to remove only the monthly back-up tape from the data center building to its designated off-site location. Contrary to District procedures, the most current daily and weekly back-up tapes were not removed to the designated off-site location. Instead, they were stored on-site in the tape vault in a locked, fire proof box.

Subsequent to our visit, the District began removing the most recent daily and weekly back-up tapes to an alternative off-site location where they were stored in a locked, fire proof box. The IT Standard Operating Procedures and IT disaster recovery plan had not been updated to reflect this change of location.

Failure to remove back-up tapes to an off-site location increases the risk that the District may not be able to timely recover all AS/400 data and programs if a disaster were to occur at the data center facility.

Recommendation: The District should update the IT Standard Operating Procedures and IT disaster recovery plan to reflect the current designated storage location for the most recent daily and weekly back-up tapes.

Finding No. 14:
Physical Security Controls

Proper security of computer systems includes measures to limit physical access to the data center to those individuals requiring access to perform their job functions. Physical safeguards are further enhanced by monitoring the access to the IT facilities.

Security to the District’s IT facilities is electronically monitored and restricted. During our initial site visit, operations staff were not consistently logging visitors to the data center. Additionally, on one occasion during our audit field work, the main door to the data center was propped open for no apparent reason. When we observed this, the IS Manager immediately closed the door.

Subsequent to our initial site visit, the District implemented several changes, including stricter controls over the logging of individuals entering the data center. Subsequent audit testing determined that operations staff were logging visitors to the data center.

Recommendation: The District should ensure that the appropriate physical security access controls are consistently followed.

PRIOR AUDIT FINDINGS

Finding Nos. 1, 3, 5 through 8, 12, and 14, noted above, included issues repeated from our prior audit report No. 03-185. 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.

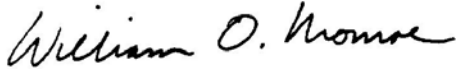
OBJECTIVES, SCOPE, AND METHODOLOGY

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 Series during the period September 2005 through February 2006. We also determined whether management had corrected, or was in the process of correcting, selected IT-related deficiencies disclosed in audit report No. 03-185.

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 7, 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 Irene Johnston, 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 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



Leading our Children to Success

201 West Burleigh Boulevard • Tavares • FL 32778-2496
(352) 253-6500 • Fax: (352) 343-0198 • www.lake.k12.fl.us

Superintendent:
Anna P. Cowin

School Board Members:
District 1
Larry Metz
District 2
Scott Strong
District 3
Becky Elswick
District 4
Jimmy Conner
District 5
Kyeleen Fischer

April 7, 2006

Mr. William O. Monroe
State of Florida Auditor General
C74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

In response to the independent auditors' Management Letter Comments relative to their audit of our Information Technology, we offer the following:

Authorization of Access

MIS will ensure that all appropriate documentation and approvals are on file for review as outlined in the IT SOP.

Emergency and Temporary Access

MIS will develop and define procedures in the SOP for Emergency and Temporary Access and will ensure that the procedures are followed.

TERMS and AS400 Access Capabilities

MIS will review with the functional owners all user access privileges during the year and the monitoring of command line access will be enhanced and restricted where possible.

Logging of Security Activity

MIS will determine if the journal will provide an adequate monitoring tool for changes to TERMS security. If this is determined to be inadequate; we will research and find a security monitoring tool within the budget available.

Terminated Employee Access

An in-house application program has been developed that the MIS Department as a whole is using to identify terminated employees directly from the HR system. As soon as an employee is flagged with a termination code by HR they appear in the list that is currently reviewed by both departments daily and appropriate action is taken. In addition, MIS has requested that HR modify the current termination form to include a check box, indicating the MIS Department has been notified by the terminating Principal or Department Head and all security has been removed for the terminating employee.

"Equal Opportunity in Education and Employment"

Other Security Controls

MIS is currently reviewing the recommended changes to determine overall feasibility; including the level of effort required to perform these corrections. Some of these recommendations will have a significant impact on the user community, some will have a significant budget impact, and at least one of the recommendations will need to be corrected by a software vendor. Once this review is completed, corrective action can be applied.

Change Management Process

The MIS Department has recently installed the Softlanding TurnOver Change Management system. This provides all proper tracking, documentation and approval of changes to the source code and the production environment. This will also provide a more updated copy of the production data available on the test machine. This will provide a more recent test environment to avoid the need for testing to replicate a problem in the production environment.

IT Standard Operating Procedures

MIS will document and review the referenced items in the department SOP as well as perform a periodic review of existing procedures and update any procedures found to be inappropriate.

PC Disposal

The District recognizes the need to properly store and prepare PCs for disposal. Procedures will be implemented to ensure hard drives are properly "cleaned" and the PCs are properly stored pending disposal.

Out-of-lease PCs

The District will correct the disposition of the PCS noted and implement procedures to ensure proper disposal methods are followed in the future for leased PCs.

Disposal Procedures

MIS will review and monitor procedures to ensure that all equipment is properly prepared for disposal. MIS has recently obtained the appropriate software to ensure proper disposal of sensitive data.

IT Disaster Recovery Plan

MIS is currently reviewing a draft sent to us from another District to provide a reciprocal agreement for back up and recovery site. This includes an annual test cycle to be performed. Once the draft has been reviewed by the Board Attorney the agreement will be presented to the Board for approval.

Back Up Tapes


MIS will update the Standard Operating Procedures (SOP) to reflect the current new locations for offsite back-up tapes.

Physical Security Controls

The IS Manager has discussed the physical security issues as referenced with the Operations staff and the custodian. There will be a periodic review of logging visitors by management to ensure proper records are being maintained.

We appreciate your assistance and review of our systems, and look forward to working together to continually improve our District.

Respectfully submitted,



Anna Cowin, Superintendent of Schools



Ken Osman, Chief Technology Officer



Tommy Crosby, Chief Financial Officer