



STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY
DEPARTMENT OF AUDIT
DIVISION OF COUNTY AUDIT
SUITE 1500
JAMES K. POLK STATE OFFICE BUILDING
NASHVILLE, TENNESSEE 37243-0269
PHONE (615) 401-7841

February 27, 2007

DeKalb County Mayor and
Board of County Commissioners
DeKalb County, Tennessee

To the County Mayor and Board of County Commissioners:

In conjunction with the annual audit of DeKalb County, we have performed a limited review of the information systems in the Offices of County Mayor, Road Supervisor, Director of Schools, Trustee, Circuit and General Sessions Courts Clerk, Clerk and Master, Register, and Sheriff as of February 6, 2007. This letter transmits the results of our review.

Our audit of DeKalb County is required to be conducted in accordance with standards contained in Government Auditing Standards, issued by the Comptroller General of the United States. These standards specify that we perform general and application control reviews of computer-based accounting and information systems to determine whether an entity's existing procedures and controls provide adequate assurance of data accuracy and financial and operating statement reliability.

Because of inherent limitations in any internal control structure, errors, irregularities, or control weaknesses may exist and may not be detected. However, our information system reviews performed in the Offices of Road Supervisor, Director of Schools, Trustee, Clerk and Master, and Register did not reveal any matters that we considered to be a reportable condition. Reportable conditions were identified in the Offices of County Mayor, Circuit and General Sessions Courts Clerk, and Sheriff. These reportable conditions may be included in the annual financial report of DeKalb County. These matters are also presented in detail in the enclosed Review of Internal Controls Regarding Information System Operations – Findings and Recommendations.

A brief summary of the reportable conditions by office is presented below:

COUNTY MAYOR

1. The office had deficiencies in computer system back-up procedures.

CIRCUIT AND GENERAL SESSIONS COURTS CLERK

1. The office did not implement adequate controls to protect its information resources.

DeKalb County Mayor and
Board of County Commissioners
February 28, 2007
Page 2

SHERIFF

1. The office had deficiencies in computer system back-up procedures.

Please contact Penny Austin, Information Systems Audit Manager, or me if you have any questions regarding our review of the information systems in the aforementioned offices of DeKalb County, Tennessee.

Sincerely,



Richard V. Norment
Assistant to the Comptroller

RVN: pa

Attachment

cc: The Honorable Kenny Edge, Road Supervisor
The Honorable Mark Wiloughby, Director of Schools
The Honorable Sean Driver, Trustee
The Honorable Katherine Pack, Circuit and General Sessions Courts Clerk
The Honorable Debra Malone, Clerk and Master
The Honorable Jeff McMillen, Register
The Honorable Patrick Ray, Sheriff
Mr. Carl Lowe, Mid-East Tennessee Audit Manager

DEKALB COUNTY, TENNESSEE
REVIEW OF INTERNAL CONTROLS REGARDING INFORMATION SYSTEM
OPERATIONS — FINDINGS AND RECOMMENDATIONS
AS OF FEBRUARY 6, 2007

The review of controls over information systems in the Offices of County Mayor, Circuit and General Sessions Courts Clerk, and Sheriff indicated a need for improvement. The following findings and recommendations have been made in order to aid these offices in the implementation of controls to better secure their computer systems and the information contained therein. These matters were reviewed with management to provide an opportunity for their response. Management offered oral responses to these items but did not submit written responses. We did not include oral responses in this report.

OFFICE OF COUNTY MAYOR

THE OFFICE HAD DEFICIENCIES IN COMPUTER
SYSTEM BACK-UP PROCEDURES

1. FINDING

The following weaknesses regarding computer system back-up procedures in the office were identified:

- A. System backups were not performed on a routine basis. Inadequate back-up procedures could result in the loss of data in the event of a hardware or software failure. Without current system backups, the cost of re-creating data could be substantial.
- B. Daily backups were not stored in a secure location. Unsecured access to system backups exposes the data to environmental hazards, as well as to possible sabotage.
- C. System backups were not stored off site. In the event of a disaster, all back-up data could be destroyed, resulting in costly delays in generating and recording information accounted for through the automated process.
- D. The back-up log did not document label descriptions, contents, and storage location.

RECOMMENDATION

Management should implement daily system back-up procedures. A backup labeled for each day of the week should be maintained. Management should store these backups in a secure, fireproof location. In addition to daily system backups, a weekly system backup should be performed, and two copies of this backup should be maintained. These backups should be rotated off site on a weekly basis. A complete systems backup should also be performed at fiscal year-end. These year-end backups should be stored off site and retained indefinitely. Some possibilities for an off-site storage location would be another county office building with a fireproof vault or a safe-deposit box at a local bank. Furthermore, a current log of all backups that includes label descriptions, date of creation, contents, and storage location should be maintained.

OFFICE OF CIRCUIT AND GENERAL SESSIONS COURTS CLERK

**THE OFFICE DID NOT IMPLEMENT ADEQUATE CONTROLS
TO PROTECT ITS INFORMATION RESOURCES**

1. FINDING

The office did not implement adequate controls to protect its information resources. This finding does not identify specific vulnerabilities that could allow someone to exploit the office's information. Disclosing those vulnerabilities could present a potential security risk by providing the readers with information that might be confidential pursuant to Section 10-7-504(i), Tennessee Code Annotated. We provided the official with detailed information regarding the specific vulnerabilities we identified, as well as our recommendations for improvement.

RECOMMENDATION

The office should ensure that adequate controls over information systems and the resources associated with those systems are implemented.

OFFICE OF SHERIFF

**THE OFFICE HAD DEFICIENCIES IN COMPUTER
SYSTEM BACK-UP PROCEDURES**

1. FINDING

The following weaknesses regarding computer system back-up procedures in the offices were identified:

- A. System backups were not performed on a routine basis. Inadequate back-up procedures could result in the loss of data in the event of a hardware or software failure. Without current system backups, the cost of re-creating data could be substantial.
- B. Daily backups were not stored in a secure location. Unsecured access to system backups exposes the data to environmental hazards, as well as to possible sabotage.
- C. Weekly and fiscal year-end backups were not performed. These backups would ensure the restoration of system data if problems occurred.
- D. System backups were not stored off site. In the event of a disaster, all back-up data could be destroyed, resulting in costly delays in generating and recording information accounted for through the automated process.
- E. A back-up log was not maintained. If system backups are not labeled and inventoried systematically, discrepancies may occur and affect the integrity of system backups in the event of a hardware or software failure.

RECOMMENDATION

Management should implement daily system back-up procedures. A backup labeled for each day of the week should be maintained. Management should store these backups in a secure, fireproof location. In addition to daily system backups, a weekly system backup should be performed, and two copies of this backup should be maintained. These backups should be rotated off site on a weekly basis. A complete systems backup should also be performed at fiscal year-end. These year-end backups should be stored off site and retained indefinitely. Some possibilities for an off-site storage location would be another county office building with a fireproof vault or a safe-deposit box at a local bank. Furthermore, a current log of all backups that includes label descriptions, date of creation, contents, and storage location should be maintained.

PRIOR AUDIT RECOMMENDATIONS NOT IMPLEMENTED

(Ref: Review of Internal Controls Regarding Information System
Operations as of February 8, 2005)

OFFICE OF COUNTY MAYOR

Finding Number	Page Number	Subject
1	1	The office had deficiencies in computer system back-up procedures

OFFICE OF SHERIFF

Finding Number	Page Number	Subject
1	2	System back-up procedures should be improved

PRIOR AUDIT RECOMMENDATIONS IMPLEMENTED

(Ref: Review of Internal Controls Regarding Information System
Operations as of February 8, 2005)

OFFICE OF SHERIFF

Finding Number	Page Number	Subject
2	2	Adequate inventory records should be maintained