Tarrant County, Texas

Report to Management
Year Ended September 30, 2004

Deloitte.

Deloitte & Touche LLP
JPMorgan Chase Tower
2200 Ross Avenue, Suite 1600
Dallas, TX 75201-6778
USA

Tel: +1 214 840 7000
www.deloitte.com

April 18, 2005

The Honorable County Judge and Commissioners Court
Tarrant County, Texas

Dear Commissioners Court and District Judges:

In planning and performing our audit of the basic financial statements of Tarrant County, Texas (the "County"), for the year ended September 30, 2004 (on which we have issued our report dated April 18, 2005), we considered its internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the basic financial statements and not to provide assurance on the County's internal control. Such consideration would not necessarily disclose all matters in the County's internal control that might be material weaknesses under standards established by the American Institute of Certified Public Accountants. A description of the responsibility of management for establishing and maintaining the internal control, and of the objectives of and inherent limitations in such controls, is set forth in the attached Appendix and should be read in conjunction with this report. A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. We noted no matters involving the County's internal control and its operation that we consider to be material weaknesses as defined above.

We did note other matters related to the County's internal control and certain other administrative and operating matters. Our observations and recommendations are presented in the attached Exhibit.

This report is intended solely for the information and use of the County Judge, the Commissioners Court, and management and is not intended to be and should not be used by anyone other than these specified parties.

We would be pleased to discuss these observations and recommendations further with you and to assist you in implementing them.

Yours truly,

Deloitte & Touche LLP

ADMINISTRATIVE AND OPERATING MATTERS

PROPERTY TAXES RECEIVABLE

Observation

The Tarrant County Tax Office (the "Tax Office") collects property taxes for entities that fall under Sections 33.07 and 33.08 of the property tax code. The County is responsible for sending out notices specifying the amount due and the date the County will begin assessing penalties. During the 2004 fiscal year, Information Technology Tax employees failed to identify and notify all properties that fall under the Section 33.08 property tax code. The County did not send out notices to the taxpayers under this code, nor did it assess penalties on these properties.

Recommendation

The Tax Office should establish procedures for the timely identification and notification of all entities that owe property taxes to the County or those entities for which the County collects taxes. The County should evaluate and properly record any penalties on delinquent collections.

Response

The Tax Office is considering several new queries whereby delinquent accounts can be identified.

RELATED PARTIES

Observation

As noted in the prior year, although the County maintains conflict-of-interest statements for the Commissioners Court and County personnel, no formal listing of related parties of Commissioners Court members or County personnel is maintained by County departments.

Recommendation

A formal listing of related parties should be prepared and circulated to County departments to ensure that any related party transactions are appropriately identified, accounted for, and approved.

Response

The County requires that its elected, appointed, and other decisionmakers follow the County's Code of Conduct, indicating whether there is a conflict of interest in a business transaction. Additionally, members of the Commissioners Court are required to sign an affidavit revealing any private interest they may have concerning an item before the Court for action. The County will continue to develop an Integrity Risk Program with the intent to establish clear expectations of County personnel and vendors as to the County's business culture. The program should provide widely distributed and acknowledged guidelines as to how the County intends to conduct its business process.

CONTRACT MANAGEMENT

Observation

The County has contracted with the North Central Texas Council of Governments ("COG") for all grant funds received from the Texas Commission on Environmental Quality ("TCEQ") by the County to be forwarded to COG within five business days from the receipt of funds. For the time frame in which the County holds the funds from TCEQ, interest income is earned that is also to be transferred to COG. On October 3, 2003, funds were received by the County from TCEQ, but the funds and earned interest income were not forwarded within the stipulated time frame to COG.

Recommendation

The County should assign the responsibility of monitoring the transfer of funds and related interest income on a timely basis. The County should explore the possibility of renegotiating the contract with COG to include an appropriate time period for the transfer to be made, if five business days is not an appropriate time frame.

Response

The County has begun discussions with COG concerning a contact amendment that will lengthen the time between the County's receipt of funds from TCEQ and the transfer of those funds to COG. We will be working with the County Auditor's Office and COG to determine the appropriate timing of funds transfer, develop an amendment to the current contract, and request Commissioners Court action to approve the amendment.

VERTEX REPORTS

Observation

The County is required to file quarterly Vertex reports to the Texas Juvenile Probation Commission ("TJPC"). During the 2004 fiscal year, the third and fourth quarter Vertex reports had not been submitted to TJPC as of March 2005, making the length of time that these reports were delinquent more than six months. Thus, delays of several months occur between the date an expenditure is incurred and the date the request for reimbursement is submitted to TJPC. Delays in submission of expenditures for reimbursement may have a negative impact on the County's cash flow.

Recommendation

The County should establish a date on which the quarter will be officially closed and implement procedures that require all adjusting journal entries to be completed and entered in the system prior to that time. A staffing analysis should be performed to review staffing levels and workload to ensure that position responsibilities maximize internal control, compliance monitoring, and utilization of personnel resources.

Response

The County's implementation of a new ERP system created a backlog of reporting. The policy has been implemented to close the month in a timely manner, which should eliminate the delay of submitting reports.

BANK RECONCILATIONS

Observation

At the fiscal year-end, the following situations were noted in the cash and investment areas:

- The County's bank reconciliation for Child Support Services included a deposit in transit that was not received by the County until after year-end. Checks that were to be paid from the incoming wire from the State were cut and held until the wire was received, and classified as outstanding checks per the reconciliation.

- The SAP payroll account reconciliation is not being prepared in a timely manner. Old checks dated back to October 2003 and other miscellaneous items were still outstanding on the bank reconciliation.

Reconciliation of bank accounts is an important element of an internal control system. A lack of reconciling bank accounts increases the risk that errors and irregularities occur and are not detected on a timely basis.

Recommendation

Procedures should be implemented that would require a supervisory review of bank reconciliations on a timely basis. Deposits in transit and outstanding checks should be reviewed to ensure that they are properly included on the reconciliation.

Response

The Auditor's office will coordinate with Child Support Services to ensure that the money from the State has been deposited prior to the issuance of checks. Since the County has completed the implementation of SAP and the manual interface has been eliminated, the payroll bank account can now be reconciled in a timely manner.

NEW ACCOUNTING PRONOUNCEMENTS

GASB 40: DEPOSIT AND INVESTMENT RISK DISCLOSURE

Observation

The Governmental Accounting Standards Board ("GASB") has issued Statement No. 40 ("GASB 40"), *Deposit and Investment Risk Disclosures*—an amendment of GASB Statement No. 3, which will be effective for the County in fiscal year 2005. GASB 40 establishes more comprehensive disclosure requirements regarding state and local governments' deposit of investment risk related to credit risk, interest rate risk, and foreign policy risk.

GASB 42: CAPITAL ASSET IMPAIRMENT

Observation

The GASB has also issued Statement No. 42 ("GASB 42"), *Accounting and Financial Reporting for Impairment of Capital Assets and for Insurance Recoveries*, which will be effective for the County in fiscal year 2006. GASB 42 requires that state and local governments report the effects of capital asset impairments in the financial statements when impairments, which are determined to be other than temporary, occur. Impairments of capital assets can occur under the following circumstances: changes in the utility of the asset,

physical damage, changes in legal or environmental laws and regulations, technological changes or obsolescence, changes in the manner or duration of use, or construction stoppages.

GASB 44: ECONOMIC CONDITION REPORTING

Observation

The GASB has also issued Statement No. 44 ("GASB 44"), *Economic Condition Reporting: The Statistical Section*—an amendment of NCGA Statement 1, which will be effective for the County in fiscal year 2007. GASB 44 changes the requirements of what must be included in the statistical Section of the County's Comprehensive Annual Financial Report, adding new schedules, eliminating selected schedules, and requiring additional disclosures on certain data included in the statistical section.

GASB 45: OTHER POSTEMPLOYMENT BENEFITS

Observation

The GASB issued Statement No. 45 ("GASB 45"), *Accounting and Financial Reporting by Employers for Postemployment Benefits Other Than Pensions*, which will be effective for the County in fiscal year 2007. GASB 45 establishes standards for the measurement, recognition, and display of other postemployment benefits expense/expenditures, related liabilities, and note disclosures in the financial statements.

GASB 46: NET ASSETS RESTRICTED BY ENABLING LEGISLATION

Observation

The GASB issued Statement No. 46 ("GASB 46"), *Net Assets Restricted by Enabling Legislation*—an amendment to GASB Statement No. 34, which will be effective for the County in fiscal year 2006. GASB 46 will help governments determine when net assets have been restricted to a particular use by the passage of enabling legislation and will specify how those net assets should be reported in financial statements when there are changes in the circumstances surrounding such legislation.

Recommendation

The County should begin reviewing GASB Statement Nos. 40, 42, 44, 45, and 46 and their implications to determine the potential impact on the County's financial statements. An approach should be developed for evaluating the effect on the County's accounting procedures, account balances, and report disclosures.

Response

The County is currently gaining an understanding of these new statements to determine their impact on the County's financial statements.

SAP LOG FILE REVIEW

Observation

A periodic "snapshot" review of the SAP log files is performed by IT Security; however, no records of the reviews are retained. In addition, the process for the daily review of the SAP log files is not formally documented. This adversely affects record retention and security risk.

Recommendations

A process should be developed and documented for the daily review of SAP log files. The logs should be reviewed for inappropriate access, failed login attempts, system configuration changes (reboots), etc. An audit trail should be maintained for up to six months that provides evidence of the log file review.

Response

A process is currently under development for the daily documentation review of the SAP log files. The intervention of the installation of a Symantec control center program will provide log aggregation and correlation. This program will facilitate the total system logging component for the review of SAP log files and will provide for continuous log monitoring and reporting, creating an audit trail that can be maintainable for at least six months of data review information. This program will be implemented and operational by the end of 2006.

INCIDENT RESPONSE PLAN

Observation

No formal, documented incident response plan is in place for responding to IT security violations identified during the log file reviews. Currently, if an incident is observed, a phone call is made to the responsible manager to discuss the cause and possible resolution to the problem. Without a more formal process for incident identification and response, there is an increased risk that data may not be processed accurately.

Recommendations

A plan should be in place that supports the formal tracking of incidents through a problem management process. A ticket should be opened and tracked through to the problem resolution. This provides a trail of notification and sign-off, and can help ensure that the incident is resolved.

Response

There is now an incident response plan in place that is doing the formal tracking of incidents as they occur. The Peregrine system is being used for any and all incidents, both for security and nonsecurity issues. This program notification system alerts all involved parties when incidents occur. All issues are immediately directed to the responsible parties involved and are tracked through problem resolution by the County's Help Desk. This process will continue to be reviewed internally by IT to ensure that the system is working effectively.

SAP SECURITY ISSUES

Observation

During our review of IT security, it was noted that numerous individuals have authorized access to the system for maintenance and control activities. The following issues were identified during our review of SAP security:

- 20 users have access to maintain the SUPER group.
- 17 users have SAP_ALL capability.
- 72 users have the ability to perform table maintenance.

- 67 users have the ability to perform financial table maintenance.
- 63 users have access to update the data dictionary.
- 63 users can open the system for changes.
- 61 users can change client settings.
- 122 users have SA38, allowing them to execute all programs.
- 63 users have SE38, allowing them to execute all programs.
- 4,843 users can manage background processing.
- 22 users can submit batch jobs using another ID.
- 108 users can submit all jobs.
- 17 users can delete all sessions.
- 23 users have access to locked transactions.
- 63 users can maintain access to programs ABAP/4 Workbench (SE38).
- 63 users have full access to ABAP/4 Workbench (SE38).
- 63 users have full access to ABAP/4 Workbench (SE11).

Recommendation

The SAP security settings should be reviewed, and authorizations should be changed so that only appropriate individuals have access to sensitive operations within SAP (i.e., BASIS and Security).

Response

It is agreed that user sign-ons have been issued in excess, but they were valid at the time this review was done. Most of the users were consultants working with SAP for the implementation of our current SAP module. Since that module is now complete, all the consultants have left, and their accesses have been closed. A further review by the BASIS Administrator is currently being done to ensure that only appropriate individuals will have access to the sensitive operations within SAP and that this area will continually be monitored closely in the future.

WINDOWS SECURITY

Observation

The following issues were identified during our review of Windows security that can increase the risk of unauthorized access:

- At the end of our testing, the administrator password had not been changed for 75 days.
- The administrator account has not been renamed.
- No "dummy" administrator account has been created.
- Logging is not active for the following:

    . Use of system accounts
    . Changes (add, remove, etc.) to user accounts
    . Changes to security parameters

Recommendation

The Windows security settings should be reviewed and changed as appropriate to ensure optimum security. These settings should be consistent with the County's security policies and procedures to ensure that they are configured according to management's intentions.

Response

The IT Security team is working diligently with the BASIS team to implement a solution that will allow consistent security guidelines to be developed and deployed that will provide optimum security to Windows. These guidelines will be in harmony with the County's present security policies. A solution will be in place by year-end 2005.

FIREWALL PASSWORDS

Observation

A process is not in place to enforce the regular change of firewall administrative passwords. There is a risk that unauthorized access could occur to the firewall from an individual with knowledge of the administrator password. Regular password changes help ensure that an individual with casual knowledge of the password will not be able to access the device once the password changes.

Recommendation

A process should be in place to change the firewall password at least every 90 days.

Response

At this time, the firewalls are under the control of the BASIS team. Strong efforts are now being made to move the administration password changes to the IT Server group. This change will guarantee a consistent administration of passwords that will mirror the policies already in place for the Active Directory and other systems at the County, thus preventing unauthorized access to critical files.

CONFIGURATION CHANGES

Observation

No formal process is in place for the approval of router and firewall configuration changes. This is particularly important when changes occur to the port and IP address filtering settings. An error made in the firewall configuration could expose the internal network to unauthorized access from the Internet.

Recommendation

A formal change process should be followed, including management sign-off for all changes to network devices that could impact the security and integrity of the internal network.

Response

The formal change control process that currently exists in the County's IT Department for all production changes will now include approval of router and firewall configuration changes. This is a formal change process that documents and records all changes to the Production environment. All changes taking place must be signed off by management.

DATA BACKUP

Observation

Our review of the backup tape management process indicated that no periodic tape restores are performed to confirm that the data was correctly backed up. Data backup procedures are useful only if the information is properly stored.

Recommendation

A test-restore of a randomly selected backup tape should be performed on a monthly basis.

Response

The Enterprise Data Recovery group has now backed up and restored all R3 data to a separate server for disaster recovery. A formal process already in place will be reviewed and changed to meet the recommendations made by Deloitte & Touche. This process will begin immediately, and policies will be reviewed, changed if necessary, and adopted by the Enterprise Data Recovery group.

MANAGEMENT'S RESPONSIBILITY FOR AND THE OBJECTIVES AND LIMITATIONS OF INTERNAL CONTROL

The following comments concerning management's responsibility for internal control and the objectives and the inherent limitations of internal control are adapted from the Statements on Auditing Standards of the American Institute of Certified Public Accountants.

Management's Responsibility

Management is responsible for establishing and maintaining internal control. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of control.

Objectives

The objectives of internal control are to provide management with reasonable, but not absolute, assurance regarding the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations.

Limitations

Because of inherent limitations in any internal control, errors or fraud may nevertheless occur and not be detected. Also, projection of any evaluation of internal control to future periods is subject to the risk that the internal control may become inadequate because of changes in conditions or that the effectiveness of the design and operation of policies and procedures may deteriorate.