DALLAS COUNTY

Management Letter

Year ended September 30, 2010

KPMG LLP
Suite 3100
717 North Harwood Street
Dallas, TX 75201-6585

March 31, 2011

Honorable County Judge and
The Commissioners' Court
Dallas County, Texas

Ladies and Gentlemen:

In planning and performing our audit of the governmental activities, the discretely presented component unit, each major fund, and the aggregate remaining fund information of Dallas County, Texas (the County) as of and for the year ended September 30, 2010, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards,* issued by the Comptroller General of the United States, we considered the County's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing an opinion on the effectiveness of the County's internal control. Accordingly, we do not express an opinion on the effectiveness of the County's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be significant deficiencies or material weaknesses, and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have been identified.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the following deficiencies in the County's internal control to be significant deficiencies:

Financial Reporting

Currently, the County's financial reporting process to prepare the Comprehensive Annual Financial Report (CAFR) is not formally documented. The current process is a manual, labor intensive process that takes a significant amount of time and requires numerous manual reconciliations and reclassifications by management to be able to appropriately convert the County's fund level financial statements to the government-wide financial statements. In

addition, there is only one employee who is involved in the process of converting the fund level financial statements to the government-wide financial statements. The combination of the lack of formal documentation of the process and the fact that it is currently performed by a single individual creates a single point of failure. This single point of failure increases the risk that if this employee was unable to perform his duties or was no longer employed by the County, the County would exhaust a significant amount of resources to produce its CAFR.

Recommendation

We recommend that management formally document the financial reporting process related to the preparation of the CAFR. The documentation of the financial reporting process should include sufficient detail to enable an individual with adequate knowledge of the GASB Statement No. 34, *Basic Financial Statements—and Management's Discussion and Analysis—For State and Local Governments*, reporting model to prepare the CAFR in a timely manner. This formal documentation would reduce the risk of a single point of failure related to the preparation of the CAFR.

Views of Responsible Officials

We agree the CAFR process is labor intensive requiring multiple reconciliations and reclassifications. The financial system supports intrafund allocations and subfund detail required by County management, which requires an extensive number of general ledger accounts to be summarized for GAAP financial reporting.

Financial analysts are assigned responsibility to affirm accuracy of Oracle system balances and reconcile system reports to CAFR footnotes. The County Auditor assumes a detailed role in reconciling and interreferencing all CAFR statements. An Accounting Manual delineating purpose and procedure for various year-end steps is updated annually and will be expanded as staff and time constraints allow.

The County Auditor's process of CAFR financial statement preparation is documented in an excel model. This model is driven by formulas and logic, which is relatively simple for an individual with the qualifications required if a replacement of the current financial audit manager becomes necessary. Financial statement adjustments for government-wide financial statements are well documented with either internal references within the excel model or with external excel documentation. As an example, external documentation includes the County debt and fixed asset "walk forward" schedules. Additionally, financial statement footnotes and exhibits while extensive would not be difficult to prepare by a CPA experienced in preparation of financial statements from either an SEC perspective or from a governmental perspective.

The County Auditor is aware of two possible software solutions for CAFR preparation which will be evaluated, additionally; options within Oracle release 12 will be evaluated as well.

Information Technology (IT)

We noted that various control deficiencies in the County's General Information Technology General Control (General IT Control) environment existed and were identified during the fiscal year 2009 audit by the previous external auditors. Based on our discussions with management and our review of management's update on the status of these deficiencies during the current year's financial statement audit, we noted that although management has made progress in developing policies and procedures to remediate some of these deficiencies, all of the deficiencies were not fully remediated as of the end of the fiscal year. We noted that management's ability to fully remediate these deficiencies has been hampered due to a combination of the following factors; turnover of key personnel within the IT department without being replaced with comparable resources, the lack of governance and effective oversight (CIO/IT director equivalent) of the IT Department during the current fiscal year, and the lack of financial resources.

The IT-related deficiencies were previously reported as individual deficiencies. However, these IT deficiencies have been categorized into two general categories in the current year: System Access and Change Management.

The following deficiencies are related to System Access:

System Access for Terminated and Transferred Users

Terminated user accounts are not being disabled from the various IT systems including Windows network, Unix, Odyssey, mainframe, and the data center access system within a timely manner. In addition, the changes to IT system access of transferred employees are not always communicated to the IT department for appropriate access modifications. The failure to remove terminated employees in a timely manner increases the risk that a terminated employee may inappropriately access the IT systems and/or execute unauthorized transactions. Similarly, if transferred employee access is not appropriately modified, these employees may have access that is not compatible with their job requirements.

Password Requirement Parameters

Strong password requirements such as minimum length and complexity have not been established for the mainframe and network systems. Strong password requirement parameters have not been configured for the Oracle database. The password parameters for the Unix system are inconsistently applied. Additionally, the Odyssey system is not configured to force the usage of strong passwords.

Periodic Review of User Access

Users' access is not formally reviewed and approved by the system owners on a periodic basis that would enable management to detect inappropriate access from terminated or transferred employees. The lack of a formal review process inhibits management's ability to review and

monitor the appropriate access levels for employees. This increases the risk that employees may inappropriately access systems or have access to information that is not appropriate given their job responsibilities.

Programmers' Access to the Production Environment

A programmer had access to production systems that support the Oracle Financial system and the mainframe system. Additionally, there is not currently a mechanism to detect all changes that are pushed into the production environment. Therefore, there is a lack of the appropriate level of segregation of duties between the program-testing environment and the production environment. This increases the risk that an inappropriate change to the financial system or mainframe may occur and go undetected.

Access to Odyssey Data Base Administrator (DBA) Function

The Odyssey DBA function is currently available to server administrators and programmers through a default account, which does not appear to have a business necessity.

Inappropriate Vendor Access

An external vendor had administrative privileges to the County's system. Additionally, two external vendors had administrator level accounts although they no longer had any business requirements to have an active account. This inappropriate vendor access increases the risk that the County's systems could be compromised.

The following deficiency is related to the IT Change Management process:

A change management control process has been implemented by the County. However, the formal documentation of this change management process is not being followed consistently. Additionally, in many instances, the changes are formally approved after the change has been implemented. The failure to obtain approval of a change prior to implementation in the system increases the risk that an inappropriate change will be implemented in the system. Although, an inappropriate change may be detected in the subsequent approval, during the time between when the change was implemented and the approval the County would be exposed to the risk associated with this change.

As previously mentioned, the deficiencies discussed above are all related to General IT Controls. General IT Controls are policies and procedures that relate to one or more applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General IT Controls maintain the integrity of information and security of data.

Therefore, these deficiencies in the General IT Controls have a pervasive impact on the County's applications and the related application controls. This includes applications that are utilized by the County to initiate, process, authorize, and or record transactions that appear in the County's

financial statements. As a result, the deficiencies in the IT controls reduce the reliability of controls that are designed to operate at the application level and thus increase the risk that an error may not be prevented or detected.

Recommendation

We recommend that management commit the resources to fully remediate the deficiencies that have been identified in the County's General IT Control environment. As these deficiencies continue to have a pervasive effect on the County's application controls that operate below the General IT Controls and increase the risk that they may possibly be circumvented, management should make efforts to remediate these deficiencies as soon as possible.

In addition to remediating the deficiencies that have been identified, we recommend that management perform an assessment of the current General IT Control environment and ensure that policies and procedures are formally documented, these policies and procedures are made available to personnel throughout the County, and continuously monitor the operational effectiveness of these policies and procedures.

Views of Responsible Officials

Dallas County recognized the deficiencies previously reported and has worked to remediate all. Some were completely remediated as soon as identified; others require process changes from other departments and/or changes in technology. With limited resources and competing priorities Dallas County is committed and will continue working on resolving all identified deficiencies.

* * * * * * *

During our audit, we noted an operational matter that is presented for your consideration. This comment and recommendation, which has been discussed with the appropriate members of management, is intended to result in other operating efficiencies and is summarized as follows:

Payment Card Industry (PCI) Compliance

The business environment that the County operates in is becoming increasingly more automated. A significant area of automation is occurring with the electronic processing of cash receipts via debit and/or credit cards. We noted that the County has plans of increasing the processing of cash receipt payments via debit and/or credit cards in the future. As a result of the sensitive nature of the information that is being transmitted during these transactions and the possibility that this information may be compromised, industry security standards have been established for organizations that are processing electronic payment transactions. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that **ALL** companies that process, store, or transmit credit card information maintain a secure environment. As a result, compliance with PCI DSS should be a goal of the County. We noted that the County does not currently have a formalized plan to ensure that it is compliant with PCI DSS.

Compliance with PCI DSS should not be considered optional and can bring major benefits to organizations of all sizes, while failure to comply can have serious and long-term negative consequences. Compliance with PCI DSS means that your systems are secure, and customers can trust you with their sensitive payment card information.

PCI DSS compliance also has indirect benefits such as:

- Helps form the basis for a corporate security strategy
- Helps identify ways to improve the efficiency of the County's IT infrastructure
- Efforts to comply with PCI DSS will make the County's better prepared to comply with other regulations (i.e., HIPAA).

The failure to be compliant with PCI DSS standards poses additional risks for the County. Those risks are as follows:

- Potential compromised customer data that negatively affects consumers, merchants, and financial institutions
- One incident of compromised customer information may severely damage the County's reputation and ability to conduct business effectively, far into the future
- Additionally, compromised customer information could lead to lawsuits, payment card issuer fines, and/ or government fines.

Recommendation

We recommend that management obtain an understanding of PCI DSS as soon as possible. In addition to obtaining an understanding of the requirements, management should perform an analysis to determine the gaps between the current IT security environment and the minimum acceptable requirements that would enable the County to be PCI DSS compliant. Finally, management should develop a detailed timeline and project plan to meet the requirements of PCI DSS. This timeline and plan should be monitored periodically to assess the County's progress toward becoming compliant with PCI DSS.

Views of Responsible Officials

Dallas County agrees and had begun working on a time line and project plan to ensure compliance with the requirements of PCI DSS 2.0.

* * * * * * *

This communication is intended solely for the information and use of management, the Commissioners' Court, others within the organization, and is not intended to be and should not be used by anyone other than these specified parties.

The County's written response to the significant deficiencies identified in our audit has not been subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we express no opinion on it.

Very truly yours,

KPMG LLP