KPMG LLP
Suite 1900
111 Congress Avenue
Austin, TX 78701-4091

Telephone 512 320 5200
Fax 512 320 5100
Internet www.us.kpmg.com

May 17, 2010

Audit Committee of Metropolitan Transit
Authority of Harris County
Houston, Texas

Ladies and Gentlemen:

We have audited the financial statements of Metropolitan Transit Authority of Harris County (the Authority), for the year ended September 30, 2009, and have issued our report thereon dated May 17, 2010. In planning and performing our audit of the financial statements of the Authority, in accordance with auditing standards generally accepted in the United States of America, we considered the Authority's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized as follows:

Information System

Access Management

Systems that have financial information are reviewed to determine if access to these systems is managed appropriately. As a result of this work we identified the following four issues:

- Three terminated employees still have active user accounts in Active Directory.
- Evidence of account approval could not be produced for three users.
- A periodic access review is not conducted to mitigate or reduce the risk of unauthorized accounts (OTS and Banner application only).
- Shared administrative accounts (Generic UNIX ID's) are being used for server administration (Banner and Oracle servers).

Risk

Without timely disablement of accounts for users after termination, there is an increased risk of unauthorized access to critical financial data. The risk for the identified terminated users is low in that these users do not have access to any of the financial reporting applications. Additionally, we noted that the access was appropriate for the three users noted above however the documentation showing the approval was not retained or could not be produced on request. Since the access was noted as being appropriate the associated risk is significantly reduced for these three users.

We noted that the IT department was not notified timely of the termination of these users and therefore the network access was not disabled timely. However, the access issues that may exist may not be identified and removed timely without a periodic review.

For shared administrative accounts, the shared user accounts carry no identity assurance and therefore tracking administrative activities back to particular individuals becomes challenging.

Recommendation

KPMG recommends that all terminated employee accounts should be removed from all systems in a timely manner. In order for this process to be effective IT should be notified of terminations in a timely and consistent manner. User accounts should not be created or modified without documentation demonstrating management approval and these approvals should be retained for auditing purposes. All administrative users should use unique accounts, owned by them, to manage and change critical systems to allow for full disclosure of identity. KPMG also recommends that employee accounts are reviewed periodically to monitor appropriateness of access on an ongoing basis. A periodic access review should be conducted to validate that functional and administrative access is appropriate.

Management Response

All accounts identified in the Audit were immediately removed and/or disabled from METRO's systems. IT will continue to work with the Human Resources Department on refining the current notification process. IT has already put into place a new User Status Monitoring System that will aid and/or eliminate untimely removal of employees from its core systems. IT has also implemented a User Access Review Process in which system owners will be able to update IT on the access status of its employees.

Programmer Access

We noted two accounts that resulted with Programmers access to development and production for OTS and Oracle Financials.

Risk

An unauthorized change could be developed and moved into production by a single individual, without following the regular change control process. This increases the risk that changes may be made without adequate testing and therefore systems may operate in a manner that is inconsistent with managements understanding and requirements.

The risk was reduced for one user as the account was disabled which prevents logon access to the OTS and Oracle Financial applications. The remaining users switched job functions and no longer required the access.

Recommendation

KPMG recommends that program changes should be implemented by personnel separate from development and that individuals should not have access to both the development and production environments. In cases that a programmer has access to both, a strong monitoring control should be in place to identify unauthorized changes to production. Further a strong access review process should be able to assist in catching personnel who have switched roles and no longer require the previously granted access.

Management Response

Neither Programmer listed above had access to METRO's systems. Both programmers access was removed when the accounts were found. As noted in the Access Management Comment above, IT has implemented and refined a User Access Review Process which should remedy or mitigate this risk in the future.

Passwords

To administer computer systems / applications, multiple levels of passwords may exist, that are transparent to most people that use the computer systems. These administration accounts / passwords normally exist at the Operating System (e.g., Windows, UNIX), Database (e.g. Oracle) and also may exist for administrators to access and modify the operation of the Applications. Administrator account and password controls are sometimes distinct to the password configurations that control how most people access the computer applications.

We noted that some of these elements were not in place at METRO (e.g., for Oracle financials, Banner and OTS), but METRO's management cannot implement additional password controls due to restrictions in the current system capabilities and without individual system customizations.

Risk

Without good controls over user accounts and passwords the risk of password compromise increases. The combination of maximum and minimum age, history, and minimum length aid in keeping the password lifetime to specific span of time, therefore, lowering the risk of password compromise, and subsequent use of that account by an unauthorized person, because the password is only valid for that specified period of time.

Having strong controls over system administration accounts and passwords is often more important as the administrators have access to modify the data directly and create / change system accounts.

Recommendation

KPMG recommends that additional stronger password requirements should be in place, where it is currently possible within the METRO environment. As systems are implemented / upgraded, passwords should be strengthened to further enhance the overall control environment.

Management Response

As noted by the auditors, IT cannot implement additional passwords control on these systems due to restrictions in the current technical capabilities of the systems. As newer systems are implemented or upgraded (e.g. SAP/HRM), the future passwords will be strengthened in accordance with IT's current complex password policy.

National Transportation Data Reporting

Management has informal procedures for reporting and maintaining data in accordance with the NTD requirements and definitions set forth in 49 CFR Part 630, *Federal Register*, January 15, 1993 and as presented in the *2009 Reporting Manual*. The lack of codified procedures may lead to challenges in preparing the required NTD report.

Recommendation:

To provide additional assurance of adhering to the accumulation and reporting of data consistent with the NTD definitions and requirements set forth in the NTD *2009 Reporting Manual*, management should implement written NTD procedures to assist the personnel assigned responsibility of supervising the preparation and maintenance of NTD data. As part of this effort, management should also seek out opportunities to improve the data accumulation and report generating process. Additional data automation in the reporting process is one area that warrants consideration.

Risk

The implementation of formal policies and procedures and the addition of data automation may reduce the risk of submitting data that is not consistent with NTD guidelines and reporting standards.

Management response:

Management agrees that codification of the informal procedures could benefit the NTD report preparation process and has already begun to develop a plan to complete codification of procedures by June 30, 2010. Implementation of the plan has started and first will entail meetings with KPMG and staff responsible for preparing and reviewing data included in the NTD report. Included in the plan are options to improve data accumulation and automation and the report generating process. Additionally management will seek ways to reflect HOV carpool ridership on the NTD report.

In addition, we identified a deficiency in internal control that we consider to be a significant deficiency, and communicated the deficiency in writing to management and those charged with governance on our report dated May 17, 2010.

* * * * * * *

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Authority's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

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

Very truly yours,

KPMG LLP