KPMG LLP
700 Louisiana Street
Houston, TX 77002

February 6, 2009

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

Ladies and Gentlemen:

We have audited the financial statements of Metropolitan Transit Authority of Harris County, Texas (METRO) for the year ended September 30, 2008, and have issued our report thereon dated February 6, 2009. In planning and performing our audit of the financial statements of METRO, we considered 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 METRO's internal control. Accordingly, we do not express an opinion on the effectiveness of METRO'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. We did not audit METRO's responses, and accordingly we express no opinion on them.

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 two issues:

- A shared administrative account was being used for OTS administration.
- A periodic access review is not conducted to mitigate or reduce the risk of unauthorized accounts.

Risk

Shared user accounts carry no identity assurance and therefore tracking administrative activities back to particular individuals becomes challenging. Inappropriate access may not be identified and removed timely without a periodic review.

Recommendation

KPMG recommends that employees' accounts are reviewed periodically to monitor appropriateness of access on an ongoing basis. User accounts should not be created or modified without documentation demonstrating management approval. All administrative users should use unique accounts, owned by them, to manage and change critical systems. A periodic access review should be conducted to validate that administrative access is appropriate.

METRO's Response

METRO does in fact utilize a shared administrative account in the OTS custom system. This account is the lynch pin account to several processes within the system and is the account that must be accessed when staff is troubleshooting a problem. METRO only has two database administrators supporting 100+ databases, so it's essential that they both know the password. As METRO continues its application consolidated process, this application will be replaced and the problem resolved.

With respect to periodic access review, IT implemented a user account review process for its major applications in October 2008. However, the audit period was prior to this implementation.

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 management can not 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. Password complexity helps to increase the difficulty in guessing / hacking a password. 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. Account lockout aids in instances of potential account password guessing by a malicious user, by locking out the account after specified thresholds.

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.

METRO's Response

METRO has put stronger password controls in where possible in these environments. METRO is limited in fully implementing these controls because they are not available in these older software versions. METRO commits to implementing strong password controls as it upgrades its systems in its application consolidation process.

Programmer Access

Programmers have access to development and production for OTS. In addition, it was difficult to produce logs to show that changes made had a corresponding change control request and approval.

Risk

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

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 where a programmer has access to both, a strong monitoring control should be in place to identify unauthorized changes to production.

METRO's Response

Segregation of duties was implemented last Spring and is an ongoing focus in IT. As soon as this particular incidence was discovered, staff corrected it.

Change Management

METRO IT has made efforts in improving the change management process around the critical applications and supporting infrastructure. An area for improvement was noted however in the retention of formal documentation outlining that appropriate testing was conducted prior to implementation of a change.

Risk

Changes could be moved into production without proper testing causing an adverse impact on the production environment.

Recommendation

KPMG recommends that program changes should be tested and the test procedures and results be documented and approved prior to being implemented into production.

METRO's Response

In the interest of continuous improvement, METRO IT has modified the change management process over the past year. The result has been significant improvement on production system changes and stability. IT will continue to give significant focus to improvement of this process, including formal documentation of end-user testing.

* * * * * * *

This report is intended solely for the information and use of the Audit Committee, management, and federal awarding agencies and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP