KPMG LLP
2001 M Street, NW
Washington, DC 20036

The Members of the Board of Directors
Washington Metropolitan Area Transit Authority:

We have audited the financial statements of the Washington Metropolitan Area Transit Authority (WMATA), for the year ended June 30, 2005, and have issued our report thereon dated September 30, 2005. In planning and performing our audit of the financial statements of WMATA, we considered internal control in order to determine our audit procedures for the purpose of expressing our opinion on the financial statements. An audit does not include examining the effectiveness of internal control and does not provide assurance on internal control. We have not considered internal control since the date of our report.

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 presented in Appendix A. Appendix B presents the current status of the prior year's management letter comments.

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 WMATA gained during our fiscal year 2005 audit 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 report is intended solely for the information and use of the Board of Directors of the Washington Metropolitan Area Transit Authority and the management of WMATA, and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

September 30, 2005

Appendix A

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Management Letter Comments

2005-01 Improvements Are Needed in Rail Revenue Cash Reconciliations and Records Retention

Observation

KPMG noted that a control related to the reconciliation of rail revenue did not contain all original documentation. In performing internal control procedures over WMATA's rail revenue reconciliation control, 13 of 15 reconciliation packages requested could not be provided in their entirety. The reconciliation package agrees the daily individual cash count to the AS400 revenue database. The Revenue Facility Center personnel were not able to provide the complete reconciliation packages for any reconciliation performed prior to June 2005 because the source documentation was not retained beyond four months. A similar issue was noted as a finding in the prior year.

Criteria

The Standards for Internal Control, established by the GAO requires that "internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained."

Cause

Management has not implemented a document retention policy that requires all original fiscal year records be retained and easily accessible as suggested in the prior year's finding. The destruction of these records erases the audit trail of management's internal control procedures.

Effect

The failure to properly maintain original records limits WMATA's ability to show that internal controls were in place and operating effectively throughout the entire fiscal year. It also reduces the auditor's ability to test the controls that were in place during the fiscal year.

Recommendation

We recommend that a document retention policy be documented and put in place to require that all original signed summary documentation be retained, which will ensure that the audit trail is maintained. These records should be easily accessible for reviews and audits. The Treasurer's Office should ensure that Revenue Facility Center personnel maintain original signed summary supporting documentation for internal controls performed during the fiscal year. If documents are not maintained, they should be electronically scanned and stored.

Management Response

Management concurs with the recommendation. Although supporting documentation can be reprinted (from the AS400 database) upon request, management agrees to keep the original WMATA treasurer's batch summary reports and the revenue summary reports signed by the supervisor effective immediately.

(Continued)

Appendix A

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Management Letter Comments

2005-02 Improvements Are Needed in Recording Accounts Payable

Observation

KPMG noted, during our search for unrecorded liabilities test work, that 6 out of 39 subsequent invoices or disbursements related to fiscal year 2005 expenses were not recorded as accounts payable. As a result, we concluded that there is an audit difference of $12,728,367 for the accounts payable balance as of June 30, 2005. This audit difference was listed on the summary of unadjusted audit differences that was provided to management.

Criteria

GASBS 34, 16.103 states that the statement of net assets and the statement of activities should be prepared using the economic resources measurement focus and the accrual basis of accounting. Revenues, expenses, gains, losses, assets, and liabilities resulting from exchange and exchange-like transactions should be recognized when the exchange takes place.

Cause

Invoices and estimates for services completed were not received by accounting prior to year-end.

Effect

The accounts payable account was understated by $12,728,367 as of June 30, 2005.

Recommendation

KPMG recommends that WMATA improve the closing process for capital items, so that the capital projects field offices will provide supporting documentation prior to closing for services completed through year-end.

Management Response

Management concurs with the finding and recommendation.

Appendix A

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Management Letter Comments

2005-03 Improvements Are Needed Related to Access Controls

Observations

- With the implementation of PeopleSoft systems, a limited auditing trail exists with the administrative privileges of the Accounting Systems Group. Inappropriate access exists in this group's administrative privilege to the PeopleSoft financial application.
- WMATA does not always deactivate and remove network user IDs and access to applications in a timely manner due to nonreceipt of information.
- Password-protected screen savers are not automatically used.
- Password policy should firmly emphasize the requirement for passwords of appropriate length to meet COBIT DS 5 IT standards for strong passwords when possible.

Criteria

Control Objectives for Information and related Technology (COBIT), released by the COBIT Steering Committee and the IT Governance Institute, requires that an organization have logical access controls that ensure that access to the systems, data, and programs is restricted to authorized users. In addition, COBIT calls for strong passwords of appropriate length.

Cause

PeopleSoft systems do not track what has changed, only who and when, allowing a limited auditing trail. The Accounting Systems Group, part of the Accounting Department, has administrative privilege due to initial setups and the need to immediately support the accounting department with access issues in PeopleSoft.

IT Services does not always receive notification from supervisors that an employee has been terminated. Additionally, HR does not notify IT Services when an employee has been terminated (per P/I. 15.07.04.06.). Without notification, IT Services has no official way of knowing that an employee has been terminated.

Password-protected screen savers are recommended but cannot be monitored. Individual users may change personal settings on their computers to activate or deactivate password protection on screen savers.

Due to older legacy systems and platforms, passwords are restricted in some situations to 4 characters. As a result, the current policy is to have passwords with a minimum of 4 characters with 6 characters recommended when possible with newer systems. The policy does not appear to firmly require a 6 character minimum when feasible.

Effect

With accounts having full administrative privileges in the Accounting department, there is a lack of an appropriate level of audit trails to track changes due to internal PeopleSoft restrictions. The ability to make changes internally within the department limits the security and ability to track whether changes were appropriate and acceptable. There is a potential for misuse in administrative power. The full administrative privilege within the department also does not allow for appropriate segregation of duties.

(Continued)

Network user IDs that are not deactivated may allow terminated employees access to potentially significant software and systems within a WMATA facility. Users with remote access that have not been removed can potentially access the system from outside and harm the network.

Screen savers that are not password protected may allow unauthorized users easy access to potentially sensitive systems and information.

Passwords to systems and software with a minimum of 4 characters are less effective and more prone to potential harm and unauthorized access than longer password requirements.

Recommendations

We recommend that the Authority restrict full administrative privileges that the Accounting Systems Group has to strictly IT Services. Formal requests should go through IT Services and no persons outside of IT Services should have full administrative abilities. A system of provisioning and de-provisioning user roles within PeopleSoft will help eliminate some of the concern of being able to support access issues in PeopleSoft. IT Services can grant restricted and limited privileges to supervisors to allow them to provision and de-provision acceptable roles based on their area of supervision to their subordinates.

Human resources should send weekly reports to IT Services in regards to employees who have been terminated. Supervisors of employees who have been terminated in unfavorable circumstances should immediately contact the appropriate IT Services staff to remove employee access.

A policy regarding password-protected screen savers should be initiated where all users are expected to use protected screen savers when away from their computer. The default setting of all newly purchased computer equipment should have a password screen saver set up.

The IT Security Policy should be updated so that a firm policy exists where all passwords are required to have 6 alphanumeric characters when possible. Passwords with fewer characters should be exceptions based on system requirements and not minimum requirements for all systems.

Management Response

Management concurs with these findings and recommendations.

ITSV and its security administration program are being revitalized to better address contemporary threats and methods, and are being updated to address expanding requirements presented by the IT Renewal Project deployment. Commensurate with this action, revised IT security job descriptions have been prepared and forwarded for evaluation by the Office of Compensation and Benefits staff. Recruitment for two vacancies will begin when the job descriptions are approved.

- During implementation of the new PeopleSoft financial software, a policy exception was authorized where security administration rights were granted to non-ITSV personnel in order for the required modifications to be made during the transition period to the new system. Various issues surrounding the functionality of the new software required these rights to be maintained. Continuous monitoring of these persons was maintained. As part of routine security monitoring, ITSV is currently reviewing the list of persons with full access rights in order to reduce and eventually eliminate full access for non-ITSV staff.

Appendix A

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Management Letter Comments

- ITSV will work with ACCT to establish the ability for supervisors to provision/de-provision access for their subordinate staff.
- ITSV will request that HRMP notify IT Security of terminated/retired employees on a weekly basis.
- All WMATA offices will be notified that ITSV Security is to be notified by the supervisor immediately upon involuntary termination.
- IT Security will include a requirement for password-protected screen savers in its current Computer Security Policy when it is refreshed.
- IT Security will work with the LAN/WAN staff to ensure that newly distributed PCs have a mandatory password-protected screen saver. IT Security will also see if it is possible to "push" a password-protected screen saver to all current users. In the interim, IT Security will notify all users of the necessity to use password-protected screen savers and include instructions on how to enable this feature.
- IT Security requires the configuration for passwords for new systems to be 6 characters, of which 2 must be numeric. When the Computer Security Policy is refreshed, it will be restated to require 6 characters and identify that exceptions can occur for legacy applications that require less.
- Beginning immediately, the Office of Human Resources Management will notify ITSV of terminated employees, so that their access may be turned off. Official notifications are often received in HR long after an employee has been terminated. Therefore, timeliness may be an issue. We will monitor this and determine if a more timely process should be identified and implemented.

(Continued)

Appendix A

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Management Letter Comments

2005-04 Improvements Are Needed Related to Service Continuity

Observations

- WMATA's Continuity of Operations Plan (COOP) should be expanded upon to include more detailed information on emergency procedures where general evacuation is not feasible.
- WMATA's procedures for nonemergencies do not include sufficient means of delivering information to employees. Currently, no intercom system is in place, requiring that in nonemergencies, instructions be delivered by telephone tree to supervisors of employees or by word of mouth on each floor.
- A plant irrigation system is located above the computer room, which is a flood risk to the computer room.

Criteria

Control Objectives for Information and related Technology (COBIT), released by the COBIT Steering Committee and the IT Governance Institute, requires that an organization make sure IT services are available as required and ensure a minimum business impact in the event of a major disruption. This includes proper development of emergency evacuation procedures.

Cause

Emergency and nonemergency response procedures are continually being developed but have not been fully implemented.

The location of the plant irrigation system to the computer room was not considered when implementing the system.

Effect

Different types of emergency situations may require different policies. Immediate evacuation is not always an option and thus situations may require different ways to be handled that may not allow for immediate evacuation.

There is a lack of immediate notification in nonemergency situations. It is possible that there will be personnel that are not available when the phone tree is started, restricting the dissemination of information or employees that may be missed during a word of mouth distribution of information.

The plant irrigation system has the potential to rupture and cause damage to the level beneath it, which happens to be the computer room.

Recommendations

We recommend that the Authority initiate a more robust written emergency response plan that considers variable plans to cover distinct situation types that may require specific ways to be handled. A general evacuation will not always be a feasible plan. An intercom system may also aid in situations where fire alarms are not activated and evacuation is not required or is restricted.

For nonemergency situations an intercom system should be implemented.

The plant irrigation system should be moved to avoid the risk of leakage and possible damage to the data center. Regular monitoring of the current irrigation system should be maintained.

(Continued)

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Management Letter Comments

Management Response

Management concurs with the findings and recommendations.

- More detailed information on emergency procedures will be included in the COOP when it is updated in October 2006.
- WMATA has developed a Shelter-in-Place brochure that instructs employees to follow instructions from Metro Transit Police. Metro Transit Police can also send an authority-wide voice mail, and e-mail to employees instructing them on nonemergency instructions.
- In January 2006, Plant Services responded to an audit report proposing that the water irrigation system piping that runs through the ceiling be re-routed around the B-1 level computer rooms. On February 3, 2006, Plant Services submitted a Facilities Engineering Request referring it to CENF. In a follow-up message, Plant Services was informed by CENF that they will conduct a constructability walkdown, develop a proposal, and find a solution to the problem.

(Continued)

Appendix A

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Management Letter Comments

2005-05 Improvements Are Needed Related to the IT Security Program

Observations

- WMATA has no IT security awareness training in place for its employees.
- WMATA's violation reports are not regularly reviewed by IT Services staff.

Criteria

Control Objectives for Information and related Technology (COBIT), released by the COBIT Steering Committee and the IT Governance Institute, requires that an IT security awareness program communicate the IT security policy to each IT user and assure a complete understanding of the importance of IT security.

Cause

Employees are not required by management or by the security policy to undergo security awareness training as part of an annual security briefing or activity. Although violation reports are produced, there is no formal requirement for them to be reviewed periodically.

Effect

Without security training in place, there is a potential for employees to have a lack of understanding regarding security and safe actions. This may result in reactive procedures to combat potential malicious intrusions. Inappropriate use may occur more frequently resulting in potential damage to the Authority.

Without regular review and monitoring of violation reports, there is a possibility that unauthorized users can systematically test the system for weaknesses. Violation reports are also an indicator of potential limitations or difficulty employees are having with the system.

Recommendations

We recommend that the Authority initiate security training for employees. Security training is a proactive measure that the Authority can take to safeguard systems and sensitive information. It will also make employees more aware of potential risks and ways to protect personal safety.

Violation reports should be consistently monitored for possible deficiencies and attacks to the system.

Management Response

Management concurs with these findings and recommendations.

- IT Security will evaluate commercial off-the-shelf security awareness programs for use at WMATA.
- Violation reporting is currently performed as part of the mainframe system administration. Policies and practices are being developed for the IT Renewal Project applications. Violation report monitoring will be made part of that practice.

(Continued)

Appendix A

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Management Letter Comments

2005-06 Improvements Are Needed Related to Segregation of Duties

Observation

WMATA's financial systems group does not have updated job descriptions that include the introduction of the PeopleSoft application.

Criteria

Control Objectives for Information and related Technology (COBIT), released by the COBIT Steering Committee and the IT Governance Institute, requires that senior management implement a division of roles and responsibilities that should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions.

Cause

WMATA has only recently transitioned its systems to PeopleSoft applications and has not completed the documentation of the job descriptions.

Effect

Without a clear and updated job description, there may not be an understanding between what is expected of the employee and what the employee is actually responsible for. Employee duties should be consistent with their duties and responsibilities. An updated job description is also necessary for the hiring of new employees as the current job function has been modified with the usage of PeopleSoft applications.

Recommendations

We recommend that the Authority update the financial systems group's job descriptions to include the PeopleSoft implementation.

Management Response

Management concurs with the findings and recommendations. WMATA will update the IT financial system group's job descriptions to reflect new PeopleSoft responsibilities by December 2006.

Appendix B

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

Management Letter Comments

2004-1 Revenue Center Documentation Retention	Repeated. See comment 2005-1.
2004-2 Cash Management	Resolved.
2004-3 Improve current disaster recovery plan	Repeated. See comment 2005-4.