

# Deloitte

Deloitte & Touche LLP  
Two World Financial Center  
New York, NY 10281-1414  
USA

Tel: +1 212 436 2000  
Fax: +1 212 436 5000  
www.deloitte.com

March 28, 2008

The Audit Committee  
Metropolitan Transportation Authority  
New York, New York

And

The Management of Triborough Bridge and Tunnel Authority  
New York, New York

Dear Members of the Audit Committee and Management:

In planning and performing our audit of the financial statements of Triborough Bridge and Tunnel Authority (the "Authority"), a public benefit corporation which is part of the related financial reporting group of Metropolitan Transportation Authority ("MTA"), as of and for the year ended December 31, 2007 (on which we have issued our report dated March 28, 2008), which contains an explanatory paragraph regarding the adopting of Governmental Accounting Standards Board Statement (GASB) No. 45, *Accounting and Financial Reporting by Employers for Post Employment benefits Other Than Pensions*, in accordance with auditing standards generally accepted in the United States of America, we considered the Authority's internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control over financial reporting.

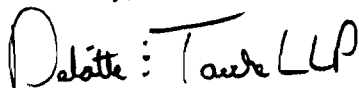
Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting. However, in connection with our audit, we identified, and included in the attached Appendix, control deficiencies related to the Authority's internal control over financial reporting and other matters as of December 31, 2007, that we wish to bring to your attention.

The definition of a control deficiency is also set forth in the attached Appendix.

Although we have included management's written response to our comments in the attached Appendix, such responses have not been subjected to the auditing procedures applied in our audit and, accordingly, we do not express an opinion or provide any form of assurance on the appropriateness of the responses or the effectiveness of any corrective actions described therein.

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

Yours truly,



## SECTION I – CONTROL DEFICIENCIES

---

We identified the following control deficiencies involving the Authority's internal control over financial reporting as of December 31, 2007 that we wish to bring to your attention:

### 1. UNIX and RAAS Application Security

***Observation:***

Security can be strengthened on the UNIX (btaixmaster) environment and the RAAS application.

***Background:***

During our assessment of the UNIX (btaixmaster) environment and the RAAS application, we identified the following areas for improvement:

*RAAS Application Security:*

1. User Access Review: A formal, documented user access review is not performed. This may result in unauthorized access if former employees or current employees that have changed job functions, have access to data they no longer need or should have access to.
2. Dormant Accounts: A former employee still had an active account within the system. This account should be made inactive to prevent unauthorized access to the application.
3. Password Controls: Currently, RAAS has the following password controls in place:
  - Passwords expiration – set to 60 days
  - Password complexity – none

However, according to the document "Technology Policy, TD014: Mainframe / Midrange Information Systems Security (7/25/00)," the following passwords controls should be implemented.

- Passwords expiration – should be set to 30 days
- Password complexity – passwords should be alphanumeric

Inconsistencies exist between documented and implemented procedures. Lack of complex passwords can increase the risk of unauthorized access due to the passwords becoming common knowledge amongst system users.

*UNIX (btaixmaster) Security:*

1. Trivial Password: The account "Oracle" has a trivial password. Weak passwords increase the risk of unauthorized access to your system and information resources. Weak password controls may also result in lack of accountability for actions performed on your system.
2. Password Controls: Currently, UNIX has the following password controls in place:
  - Password Expiration – none
  - Password Length – 6
  - Password History Size – 6

**SECTION I – CONTROL DEFICIENCIES (continued)**

---

However, according to the document “Standard Operating Procedure for IBM AIX 5.2.0,” the following passwords controls should be implemented.

- Password expiration – should expire after 4 weeks
- Password length – should be 8 characters
- Password history size – should be 20

Inconsistencies exist between documented and implemented procedures. Weak passwords increase the risk of unauthorized access.

3. Backup Tapes: Backup tapes are being sent to Randall’s Island for storage on a daily bases. However, documented evidence of this could not be obtained in 4 instances out of the 15 samples tested. Since tapes are being sent daily, documentation should be complete and provide evidence that the tapes have been received by the appropriate party at Randall’s Island. Without appropriate evidence, it cannot be determined if the tapes were received at Randall’s Island.

***Recommendation:****RAAS Application Security:*

1. User Access Review: Management should consider developing a formal process to review user’s access to RAAS at determined intervals to prevent unauthorized individuals from having access to sensitive data.
2. Dormant Accounts: Management should consider deactivating access for the former employee’s account to prevent unauthorized access to the system. Management should consider further strengthening procedures to ensure timely deactivation of access for terminated employees.
3. Password Controls: Management should consider enforcing the documented procedures around password controls. RAAS passwords should be modified to match the requirements of the *Technology Policy, TD014: Mainframe / Midrange Information Systems Security*. Per this document, the RAAS passwords should be made to expire after 30 days and the passwords should be alphanumeric.

*UNIX (btaixmaster) Security:*

1. Trivial Password: Management should consider changing the password to the account “Oracle” such that it does not equal the username. The password should be changed to a more complex and less easily guessed password to prevent unauthorized access within the UNIX system.
2. Password Controls: Management should consider updating the documented procedures in *Standard Operating Procedure for IBM AIX 5.2.0* to match desired system settings. Alternatively they should consider changing UNIX (btaixmaster) password requirements to:
  - Password expiration – 4 weeks
  - Password length – 8 characters
  - Password history – 20 passwords

**SECTION I –CONTROL DEFICIENCIES (continued)**

---

This will prevent inconsistencies between documented and implemented procedures.

3. Backup Tapes: Management should consider storing notices from Randall's Island confirming that tapes have been received. The log used to monitor the sending and receiving of tapes should be reviewed weekly to check that all tapes have been sent and received as appropriate. This will help to monitor the process of sending backup tapes and allow management to be informed quickly if a tape was not received at Randall's Island and is missing.

***Corrective Action Taken***

The following corrective action was taken based on our observations.

Dormant Accounts: The account has been changed to inactive on December 20, 2007 on the RAAS system.

***Management's Response:******RAAS Security:***

1. This will be done twice a year and was recently done in the 4th quarter of 2007. The Revenue Management Team ("RM") will issue a procedure on how this will be done.
2. RM will deactivate access immediately for all former and terminated employees. This will be the existing policy as staff leaves the department. However, RAAS does not allow RM to "delete" former employees. Accordingly, there is a "User" list of RM employees going back almost 20 years. RM will require Technology Department ("TD") assistance to at least once a year have retired and obsolete employees removed from the User list.
3. RM agrees and will need TD assistance to implement the password control upgrade. Setting password to expire in 30 days is feasible within the application. However to enforce password complexity such as to comply with alphanumeric passwords, RAAS logic has to be modified because of the limitation in the custom application.

***Unix Security:***

1. "Oracle" id is used to link the users to the shared folder in Unix. We will strengthen the password so that it can't be easily guessed. This will be done by 4<sup>th</sup> quarter 2008 at the time when the new server is deployed with Oracle 10g. However currently there is no risk as no one can directly login to Oracle.
2. These ID's are only used in FTP scripts in batch mode and therefore no direct user logins take place and no user knows these passwords. Therefore we have decided not to expire the passwords. Also changing the password to have a length of 8 characters will result changing passwords in all the FTP scripts used by ACS (customer service), Casetta (EPH servers) and the BCC (money room). This will have a major impact on day to day operations of the systems.

**SECTION I – CONTROL DEFICIENCIES (concluded)**

---

Therefore the business reasons prohibit us changing the passwords as recommended. However we will update the standard operating procedures to note these exceptions.

3. We will review weekly the log to check that all tapes have been sent and received as appropriate. The situation cited was an isolated incident where both the primary and the secondary persons responsible for maintaining the documentary evidence were out for those days and therefore could not complete the paper transactions. However backups were taken and were sent off-site as scheduled.

**SECTION II – OTHER MATTERS**

---

Our observations concerning other matters related to operations that we wish to bring to your attention are as follows:

**1. Financial Closing & Reporting Policies**

***Observation:***

Written policies do not exist outlining the procedures that need to be followed during the financial closing and reporting process.

***Background:***

During control testing it was noted that management has developed a process for financial closing and reporting which employees adhere to, however, such policies do not exist in a written format and such procedures are only communicated verbally. Written policies have not been created due to the high retention of accounting personnel and the fact that all individuals involved in the closing and reporting process are familiar with their responsibilities.

***Recommendation:***

It is highly recommended that management create formal written policies related to the procedures involved during the financial closing and reporting process which will help ensure that the controls currently in place will continue to be followed even in the unlikely event of high turnover. In addition, this will allow employees a process by which controls can be researched if questions arise as to how a policy should be performed and will help to ensure best practices are being followed. These policies should be updated on a periodic basis.

***Management's Response:***

Formal written procedures for the closing and reporting process will be prepared for the year ending December 31, 2008.

**SECTION III – PRIOR YEAR COMMENTS (2006) – OTHER MATTERS**

---

Our observations concerning other matters related to prior year's operations that we wish to bring to your attention are as follows:

**1. Information Security**

***Observation:***

Security can be strengthened on the Macola application.

***Background:***

During our assessment of the Macola application, we identified the following areas for improvement:

Password complexity has not been set for the Macola application and users are not prohibited from using generic dictionary words as passwords. This can result in the use of simple passwords that can be easily cracked by intruders and a potential risk of intruders gaining access to the system.

***Recommendations:***

Management should consider enabling password complexity for Macola. This could prevent intruders from gaining access to the system.

***Management's Response (2006):***

Macola is a commercially available off-the-shelf-system and inherits certain limitations when it comes to strengthening passwords and implementing other complex security standards. However, a new version of Macola is now available and it appears to be providing capability to implement complex security policies. The Technology Department ("TD"), working together with the Finance Department, is planning to upgrade Macola to this version by the end of 3rd quarter and implement password complexity and account lockout features as permitted by the new release.

***Status Update (2007):***

This issue has not been resolved. The upgrade to a new version of Macola did not occur.

We reiterate our comment from prior year and this issue is still open.

***Management's Response (2007):***

Due to the shared services and the Business Service Center initiative for the financial systems the upgrade was put on hold. Their recommendation was not to spend any money on upgrading legacy systems. However Technology Department in conjunction with the Finance Department will re-visit and re-evaluate the issue and decide whether this can be done in 2008.

**SECTION IV – DEFINITIONS**

---

The definition of a control deficiency that is established in AU 325, *Communicating Internal Control Related Matters Identified in an Audit*, is as follows:

A *control deficiency* 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 misstatements on a timely basis. A deficiency in *design* exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that even if the control operates as designed, the control objective is not always met. A deficiency in *operation* exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

\* \* \* \* \*