

# ***The Metropolitan Transportation Authority***

**Report to Management**

***Year Ended December 31, 2009***

April 26, 2010

The Audit Committee  
Metropolitan Transportation Authority  
New York, New York

And

The Management of the Metropolitan Transportation Authority  
New York, New York

Dear Members of the Audit Committee and Management:

In planning and performing our audits of the consolidated financial statements of the Metropolitan Transportation Authority and of the financial statements of the First Mutual Transportation Assurance Company, Long Island Rail Road Company, Metro-North Commuter Railroad Company, Metropolitan Suburban Bus Authority, MTA Bus Company, New York City Transit Authority, Staten Island Rapid Transit Operating Authority and the Triborough Bridge and Tunnel Authority (collectively the "MTA") as of and for the year ended December 31, 2009 (on which we have issued our reports dated April 26, 2010), in accordance with auditing standards generally accepted in the United States of America, we considered the MTA'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 MTA's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the MTA's internal control over financial reporting.

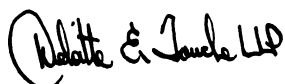
Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting. However, in connection with our audits, we have identified, and included in the attached Appendix A, deficiencies related to the MTA's internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention.

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

Although we have included management's written response to our comments in the attached Appendix A, such responses have not been subjected to the auditing procedures applied in our audits 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.

Sincerely,



**THE METROPOLITAN TRANSPORTATION AUTHORITY  
TABLE OF CONTENTS**

---

	<u>Page</u>
<b>APPENDIX A</b>	
Metropolitan Transportation Authority- Headquarters	5
First Mutual Transportation Assurance Company	18
Long Island Rail Road Company	20
Metro-North Commuter Railroad Company	24
Metropolitan Suburban Bus Authority	27
MTA Bus Company	30
New York City Transit Authority	37
Staten Island Rapid Transit Operating Authority	48
Triborough Bridge and Tunnel Authority	51
Prior Year Comments Addressed	57
<b>APPENDIX B</b>	
Deficiency Definition	61

## **APPENDIX A**

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS**

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
CURRENT YEAR COMMENTS- 2009**

---

**DEFICIENCIES**

We identified, and have included below, deficiencies involving the Metropolitan Transportation Authority- Headquarters' (MTA or MTAHQ) internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention:

**1. Classification of Long-Term Debt**

***Observation:***

Long-term debt was incorrectly classified between current and noncurrent.

***Background:***

During testing of long-term debt, it was noted that the interest rate on MTA Transportation Revenue Bonds, Series 2005A set to mature on November 15, 2026 and insured by MBIA Insurance Corporation, will increase from 3.4% to 4.0% on November 16, 2010 according to the Official Statement. Per discussion with the MTA Treasury Department, the PeopleSoft system will not allow for changes in interest rate on the bonds, therefore, the MTA Treasury Department set the maturity date of the bonds to November 15, 2010 and re-entered the bonds in PeopleSoft with the revised interest rate and correct maturity date. The accounting department ran a debt report and noted the bonds had a maturity date of November 15, 2010 and as a result recorded the entire amount as current at December 31, 2009. However, this was not the case and \$71,750,000 was reclassified from current to noncurrent.

***Recommendation:***

The Treasury and Accounting departments should communicate during the year-end and quarterly closing process to ensure that classifications between current and noncurrent for both debt and investments is correctly reported in the financial statements.

***Management Response:***

Management agrees with the recommendation. However, the misclassification was due to a unique modality of the 2005A series for the Transportation Bonds. In order to provide correct classification for such items, the Comptroller Group has implemented a review and sign off process/procedure. The sign off procedure will provide an agreement and reconciliation among the effected groups. The 1<sup>st</sup> and 2<sup>nd</sup> quarter 2010 has been reconciled and reclassification has been completed.

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
CURRENT YEAR COMMENTS- 2009**

---

**2. Classification of Investments**

***Observation:***

Investments were incorrectly classified between current and noncurrent.

***Background:***

Investments maturing within one year of December 31, 2009 should be classified as current on the balance sheet. Investments not maturing within one year of December 31, 2009 should be classified as noncurrent on the balance sheet.

It was noted that certain MTA investment securities were classified as current/noncurrent based on when the MTA planned to use the funds and not based on the maturity dates of the investment securities.

During 2009, it was requested that the MTA classify investments as current/noncurrent based on maturity dates instead of usage. As of December 31, 2009, the MTA didn't classify every investment as current/noncurrent based on the maturity date. Therefore, an audit adjustment was proposed and recorded by MTA in the amount of \$1.2 billion.

***Recommendation:***

The MTA should review the investment security detailed schedule on a quarterly basis and record all investments maturing within one year of the balance sheet date as current and all investment not maturing within one year of the balance sheet date as noncurrent.

***Management Response:***

Management agrees with the recommendation. Therefore, as in the previous recommendation, the Comptroller Group, has instituted a review and sign off process/procedure. The sign off procedure will provide a required agreement and reconciliation among the effected groups. The 1<sup>st</sup> and 2<sup>nd</sup> quarter 2010 has been reconciled and the procedure has been implemented.

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
CURRENT YEAR COMMENTS- 2009**

---

**3. Interagency Loan**

***Observation:***

An interagency loan between the Capital Financing Fund and the Operating Fund in the amount of \$500 million has been outstanding since 2002.

***Background:***

In 2002, the Transportation Capital Project Non Bond Proceed Account loaned \$500 million to the Operating Fund to pay for operating needs of the Commuters and New York City Transit Authority (“NYCTA”).

Each year the \$500 million is repaid to the Transportation Capital Project Non Bond Proceed Account and subsequently re-loaned to the Operating Fund. As of December 31, 2009, the MTA General Fund Account and the NYCTA Stabilization Account had outstanding loans of \$400 million and \$100 million, respectively, from the Transportation Capital Project Non Bond Proceed Account.

***Recommendation:***

MTA management should develop a plan that outlines the repayment of the \$500 million loan to the Transportation Capital Project Non Bond Proceed Account from the MTA General Fund Account and NYCTA Stabilization Account.

***Management Response:***

Management agrees with the recommendation. Therefore, the MTA will put a plan together in order to repay the \$500 million dollar loan to the Transportation Capital Project Non-Bond proceed account from the General Fund Account in the amount of \$400 million and the NYCTA Stabilization Account of \$100 million during 2010.

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
CURRENT YEAR COMMENTS- 2009**

---

**4. Investment Funds and Cash Accounts**

***Observation:***

New investment funds and cash accounts need to be reviewed and monitored by MTA Management.

***Background:***

The MTA portfolio is comprised of many funds. Some funds are legally restricted for specific purposes while others are not. There are certain funds, while restricted for a purpose, have the ability to make loans to other funds like the Triborough Bridge and Tunnel Authority Necessary Reconstruction Reserve and Merrill Lynch Fuel Hedge Accounts.

***Recommendation:***

MTA Management, including members of the Comptroller's Department, Treasury, In-house Legal Counsel, and Finance in conjunction with external legal counsel need to review all investment funds and cash accounts when they are first opened and determine if the funds are legally restricted or not and whether loans may be taken against any of these investment funds or cash accounts. This process should be documented in writing.

***Management Response:***

Management agrees with the recommendation. Therefore, a process has been implemented to review each new investment and cash account, with the Comptroller and MTA Bond Counsel. Thereafter, the legal interpretation related to the nature of the investment/cash definition of whether it is restricted or can be used as loan will be reconciled with the Treasury/Finance group as the account is opened. The accounts have been reconciled and the process has been implemented as of the 2<sup>nd</sup> quarter 2010.

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
CURRENT YEAR COMMENTS- 2009**

---

**5. Schedule of Federal Expenditures Reconciliation**

***Observation:***

MTA is not reconciling amounts reported as expenditures for Federal grant programs to the financial statements.

***Background:***

Adjustments made to the general ledger accounts for grant programs are not being reviewed and approved by the Revenue Department in a timely manner. Consequently, such adjustments are not always reflected in the Schedule of Expenditures for Federal Awards. A reconciliation of the amounts recorded in the financial statements to those reflected in schedule of expenditures is not being performed by management.

***Recommendation:***

MTA management, in conjunction with the Treasury, Revenue and Accounting Departments, should maintain appropriate financial records that support the amount of expenditures for grant programs recorded in the financial statements to those reported in the Schedule of Expenditures of Federal Awards. Also, all adjustments to grant program expenditures should be reviewed and approved by the Revenue Department. A reconciliation should be performed in a timely manner to ensure that all grant program transactions are captured in the Schedule of Expenditures of Federal awards.

***Management Response:***

Management has agreed with the recommendation and has implemented a process and procedure to assure that a reconciliation is completed on a monthly basis. The procedure has a sign off process by key staff for the Treasury and the Revenue/General Ledger groups. The procedure has been implemented in the second quarter, 2010.

## **6. Impact Application Password Configuration**

### ***Observation:***

No password parameters were configured at the Impact application level for password age, password history, and password complexity.

### ***Background:***

Due to the current version the impact application is running on, the system does not have the capability to enforce password settings for password age, password history, and password complexity. It was noted that the Impact application did not undergo a system upgrade to address the issue due to resource limitations.

### ***Recommendation:***

#### **1. Password Age:**

Users who access the impact application should be systematically forced to change their passwords on a periodic interval. Management should consider setting maximum password age to 90 days.

#### **2. Password History:**

Users who access the impact application and must change their password after a pre-determined amount of days should not be able to use a number of previously used passwords. Management should consider setting maximum password history to 5.

#### **3. Password Complexity:**

Easy to guess passwords lead to a risk of unauthorized access to the system. Management should consider setting more complex passwords (e.g. use of at least one character, one number, and one special character).

### ***Management's Response:***

Management agrees with the recommendation, however, the MTA acknowledges that the IMPACT application does not currently have available mechanisms to enforce password age, password history or password complexity. We have identified options to compensate for the application's shortcomings. Such options include Weblogic 10, Oracle Identify Manager, and/or an in-house password security module. The implementation of these related projects to address password safeguards are significantly influenced by 2010 budget restrictions and other resource constraints and, thus, are expected to begin no earlier than 2011.

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
CURRENT YEAR COMMENTS- 2009**

---

**7. PeopleSoft Security Violations Report**

***Observation:***

Security violation reports at the PeopleSoft application level are currently not being generated and reviewed.

***Background:***

It was noted via inquiry with Business Service Center Security that security violation reports including failed login reports and privileged access monitoring are currently not being generated or reviewed for the PeopleSoft application.

***Recommendation:***

Systems or monitoring tools should be in place and configured to capture security violations including failed logins and privileged access to logs. Those logs should be generated and reviewed on a periodic basis to check for any unauthorized activity.

***Management's Response:***

The current version of PeopleSoft does not generate failed login reports. It, however, does leverage an automatic lockout after five failed attempts. To address those accounts that are disabled due to excessive login attempts, users are required to call the Help Desk to unlock them.

Additionally, the owners of business applications (i.e., Finance, HR, and Procurement) may request privileged access reports on an exception basis. These reports provide information about changes to user profiles, role access and permission lists. They also serve as a check-and-balance mechanism to the business process.

In January 2011, an interagency system will replace the current PeopleSoft system. To mitigate risks of unauthorized access, this newer system's security configuration will reduce automatic lockout from five to three failed attempts. Also, the MTA is reviewing logging and reporting capabilities of a proposed single sign-on solution to determine what additional ID protection is feasible.

To coincide with the January 2011 upgrade, the MTA is enhancing its process and procedures to include regular monitoring of security change activity. Because of the development effort needed to implement this system, remediation of this finding should be deferred until the new PeopleSoft system is released to production.

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
CURRENT YEAR COMMENTS- 2009**

---

**8. Impact and PeopleSoft Application User Access Termination**

***Observation:***

5 terminated users continued to have active application IDs within PeopleSoft or Impact.

<b>ID</b>	<b>Application Access</b>
090318	PeopleSoft Financials and HR
103811	Impact
011569	Impact
86223	PeopleSoft HR
103838	Impact

***Background:***

To test the process of user access termination, we compared the list of terminated users to the active accounts in PeopleSoft and Impact. It was noted that there were 5 terminated users with active application accounts.

***Recommendation:***

Management should consider disabling a terminated user's access in a timely manner, unless there is a business reason to keep the account active. Not doing so leads to a risk of unauthorized access to the system and data.

***Management's Response:***

*PeopleSoft accounts:*

In January 2011, the interagency PeopleSoft system will implement an automated ID lockout and deactivation process to replace the manually implemented lockout and deactivation process in the current PeopleSoft system.

The following remarks address the specific accounts:

John Murphy:

ID "jmurphy" which is associated with employee ID 090318 is locked in all environments and clearly marked "T2009" with a last update date/time of May 14, 2009 at 15:27. Whenever an account is locked out, the "last update" date is changed to the current date. (Another John Murphy has an account named jmurphy, which is associated with employee ID #103160. This account remains active (last access May 14, 2010).

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
CURRENT YEAR COMMENTS- 2009**

---

**8. Impact and PeopleSoft Application User Access Termination (continued)**

Henry Mullaney:

Access for ID hmullane is controlled by the PeopleSoft Portal. This ID is locked in the PeopleSoft Portal. Therefore, ID hmullane is inactive throughout the HQ PeopleSoft system.

*IMPACT accounts:*

As part of business processes, Human Resources updates information about employee termination within the PeopleSoft system. These changes within PeopleSoft generate notifications to the IMPACT account administrator. The account administrators also perform regular review of active accounts.

To improve lapses and oversights, another IMPACT account manager will be added to the termination notification list. Additionally, IMPACT account managers will notify MTA Enterprise Security of the results of routine IMPACT recertification.

Steven R. Bennett and Yvonne Perry:

In the cases of Steven Bennett and Yvonne Perry, the PeopleSoft system sent out termination notifications. The failure to disable these accounts upon notification is due to human error and has been corrected.

Amit Priyadarshi

The remaining IMPACT user, Amit Priyadarshi, is currently a consultant who requires access to IMPACT.

As the report that Deloitte received cites, Priyadarshi ended his initial engagement at the MTA as a contingent employee on December 5, 2009. As part of the business process, this change generated a PeopleSoft termination notification. MTA Capital Construction later hired Priyadarshi as a consultant, who, as part of his current duties, requires IMPACT access and is therefore still active in the system.

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
PRIOR YEAR COMMENTS- 2008**

---

**1. Capital Project Receipts are not Credited to the Proper Accounts Receivable General Ledger Account**

***Observation:***

Funds are received related to capital projects that are not credited to the proper accounts receivable general ledger account resulting in negative general ledger balances as of December 31, 2008.

***Background:***

During testing of Capital Project receivable accounts, it was noted that funds received by the Treasury Department are not always credited to the proper receivable general ledger account, resulting in negative balances in and/or incorrect credits to the receivable accounts.

***Recommendation (2008):***

MTA management in conjunction with the Treasury, Revenue and Accounting departments should develop a standard template for entries involving funds received for capital projects to ensure that the receipts are credited to the proper general ledger account(s).

***Management Response (2008):***

MTA Headquarters' (MTAHQ) management agrees with the comment. However to clarify, MTAHQ has accounted for all Capital Project receivables which were actual miscodings for 2008. In regard to the audit recommendation, the MTAHQ General Accounting and Revenue groups have implemented a procedure complete with templates to correct the function. The implementation date was as of March 1, 2009.

***Status Update (2009):***

This issue has not been resolved. We reiterate our comment from prior year and this issue is still open.

***Management Response (2009):***

Management agrees with the recommendation. The process has been implemented and while the process was in place at the time of the audit, the Comptrollers' group had not provided the reconciliation on a timely basis. As of the first quarter, the Receivables have been properly credited.

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
PRIOR YEAR COMMENTS- 2008**

---

**2. No Review of Receivable Accounts**

***Observation:***

A number of accounts receivable balances recorded in the general ledger were negative as of December 31, 2008. Management does not perform a review of these account balances after the close of the accounting period to determine if the balances are appropriate.

***Background:***

During testing of accounts receivables, it was noted several general ledger accounts, as detailed below, had negative balances as of December 31, 2008. Prior to testing management had not performed account analyses to determine if the balances in these accounts were appropriate. As a result of testing management booked audit adjustments of approximately \$12,695,000.

<b>DESCRIPTION</b>	<b>ACCOUNT</b>	<b>12/31/08 BALANCE</b>
REC FR NEW YORK CITY HUDSON YD	132101	\$(8,854,636)
DUE TO CDOT	133006	(6,239,525)
REC NYS CAP PROJ - TA	131102	(6,043,000)
REC FIX ASSET NASSAU CTY-LIB	132570	(2,880,201)
REC FED GRANTS UMTA SPEC PROJ	130103	(1,223,960)

***Recommendation (2008):***

The MTA should adopt a post-closing procedure to review and analyze negative balances in the receivable accounts to determine if the credits to these receivable accounts are proper. These reviews and analyses should be performed prior to the start of the annual audit.

***Management Response (2008):***

MTA Headquarters' (MTAHQ) management agrees with the recommendation. MTAHQ General Accounting has developed and implemented a post closing procedure to review any negative balances for accounts receivable or payables as of March 15, 2009. However, due to the complexity of many of the accounts, analyses may carry through the audit start. In addition, management will provide a report to the independent auditors of any continuing analysis for on-going post closing balances by the 15<sup>th</sup> of quarter end.

**METROPOLITAN TRANSPORTATION AUTHORITY- HEADQUARTERS  
PRIOR YEAR COMMENTS- 2008**

---

**2. No Review of Receivable Accounts (continued)**

***Status Update (2009):***

During testing of accounts receivables, it was noted several general ledger accounts, as detailed below, had negative balances as of December 31, 2009. Prior to testing management had not performed account analyses to determine if the balances in these accounts were appropriate.

<b>DESCRIPTION</b>	<b>ACCOUNT</b>	<b>12/31/09 BALANCE</b>
STATE AND GRANTS RECEIVABLE	130111	\$(31,244,557)
DUE TO CDOT	133006	(6,239,525)
REC FIX ASSET NASSAU CTY-LIB	132570	(1,441,658)
REC FED GRANTS UMTA SPEC PROJ	130103	(1,429,034)

This issue has not been resolved. We reiterate our comment from prior year and this issue is still open.

***Management Response (2009):***

Management agrees with the recommendation and has used the implemented procedure to analyze and reconcile open receivable accounts. However, while the process has been successful, the General Accounting group has not provided the reconciliation on a timely basis for 2009. As of the 2<sup>nd</sup> quarter 2010, all of the above identified receivables have been reconciled.

**FIRST MUTUAL TRANSPORTATION ASSURANCE COMPANY**

**FIRST MUTUAL TRANSPORTATION ASSURANCE COMPANY  
CURRENT YEAR COMMENTS- 2009**

---

**DEFICIENCIES**

We identified, and have included below, deficiencies involving the First Mutual Transportation Assurance Company's (FMTAC) internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention:

**1. Escrow Account was not Updated for Received Wire Transfers**

***Observation:***

FMTAC did not initiate communication to obtain sufficient knowledge about an interagency transaction.

***Background:***

During testing of the escrow account, it came to our attention that the amount held in FMTAC's escrow account, as required by Metro-North Commuter Railroad Company, was not accurate. In addition, the escrow balance disclosed in the footnotes to the financial statements was not updated in 2009. A wire transfer was sent to FMTAC by Metro-North Commuter Railroad Company during 2009 which should have reduced the escrow balance held by FMTAC. This finding resulted in an adjustment proposed by D&T and recorded by FMTAC during the December 31, 2009 audit.

***Recommendation:***

All payments received from other agencies should be investigated in order to record the transaction within the proper account. Overall, communication between the agencies should be improved in order to avoid interagency transaction misstatements.

***Management Response:***

Management agrees with the recommendation and will investigate all payments received from the agencies to ensure proper accounting. Management will work to improve communication between agencies to avoid future transaction misstatements.

**LONG ISLAND RAIL ROAD COMPANY**

**LONG ISLAND RAIL ROAD COMPANY  
CURRENT YEAR COMMENTS- 2009**

---

**DEFICIENCIES**

We identified, and have included below, deficiencies involving the Long Island Rail Road Company's (LIRR) internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention:

**1. Oracle Database Passwords**

***Observation:***

We inspected the contents of 'dba\_users table' which displayed Oracle password settings. It was noted that passwords were encrypted; however passwords for user accounts were not set to expiration. No evidence was provided to show that password complexity and minimum length settings were in place.

***Background:***

'Password Lockout Date' and 'Expiry Date' was blank in the 'dba\_users' table.

***Recommendation:***

Management should configure password settings for complexity, minimum length, expiration and lockout at the Oracle Database level per the standards defined in the MTA Information Security policies.

***Management's Response:***

Management agrees with this observation. Oracle password settings were changed as requested in the first quarter of 2010.

## **2. PLS application security**

### ***Observation:***

One developer had Admin access to PLS application. Management confirmed that this access was not necessary. We noted that the PLS application currently does not have security logs to monitor application access.

### ***Background:***

It was noted that one developer was assigned admin access to PLS application. Also, there are no security logs to monitor access to the application.

### ***Recommendation:***

Management should consider removing the developer's access to PLS production. Developers can be assigned read-only access or a temporary ID (with temporary passwords) in case of a business need to access production.

Further, management should consider generating and reviewing security logs or reports showing user's access to the application. This will act as a detective control to make sure that only appropriate users have accessed the application.

### ***Management's Response:***

The Admin access to PLS for the developer will be removed in April 2010. The Human Resource Department provides a daily listing to the Information Technology (IT) Security section that reports changes to an employee's status and/or department. IT Security reviews the changes with the employee's manager to recertify/modify/remove system access as needed. Additionally, a recertification of system access is performed annually. Management believes these controls are adequate.

## **1. RSMS and CSS Database Security**

### ***Observation:***

Database Administrators (“DBA”) do not use individual user IDs to access the Oracle database for RSMS and Central Support System (“CSS”) applications. Also, there were no password parameters set for the shared ids.

### ***Background:***

Five DBAs currently have access to the Oracle database for RSMS and CSS. All five DBAs use two shared user IDs to login to the system. This can lead to a lack of accountability for changes made to the database. Also, there are no password parameters for these IDs and the passwords to these accounts have not been changed in several years.

### ***Recommendation (2008):***

Management should consider assigning separate database IDs for the DBAs in order to establish accountability to the changes made to the database. Management should also consider implementing password parameters for the database accounts to protect the data within the system.

### ***Management’s Response (2008):***

Management agrees with this recommendation however based on the criticality of these two systems will proceed cautiously with implementation. The RSMS system is supported by old technology and the CSS system is a critical revenue generating system for the MTA LIRR. Any interruption or loss of service for any period of time could have a detrimental effect on the operation of the MTA LIRR.

The DBA staff is in the process of testing the effects of having individual privileged DBA accounts in the test databases for these two systems. These changes will be evaluated and made in production once it is determined there will be no adverse effects.

### ***Status Update (2009):***

The issue for RSMS has not been resolved. The functionality for RSMS will be moved to the CAMS application, which will then resolve the issue. The issue for CSS has been resolved when the database was upgraded to Oracle 11G.

### ***Management’s Response (2009):***

Management agrees with the audit requirement. However, the RSMS application remains supported on old hardware, software and database release level. The functionality provided by RSMS is scheduled to be moved to the CAMS application by January 2011.

The CSS application (name changed to TSS) database with supporting hardware was upgraded during the first quarter of 2010. As a result of this upgrade to Oracle 11G, each DBA has an assigned user account. The shared ID’s will incorporate the use of enhanced passwords for added security.

**METRO-NORTH COMMUTER RAILROAD COMPANY**

**METRO-NORTH COMMUTER RAILROAD COMPANY  
CURRENT YEAR COMMENTS- 2009**

---

**DEFICIENCIES**

We identified, and have included below, deficiencies involving the Metro-North Commuter Railroad Company's (MNCR) internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention:

**1. *Maintenance Of Way Non-stock Inventory - Structures & Communications at Harmon***

***Observation:***

Inventory items at the Harmon warehouse location are not accounted for in the PeopleSoft inventory system. In addition, inventory items at this location are not tagged with item number identifiers.

***Background:***

Maintenance of Way non-stock inventory items at the Harmon Warehouse location are accounted for in a spreadsheet which is outside of the PeopleSoft inventory system. In addition, no item number identifiers have been assigned to these inventory items.

***Recommendation:***

Since it is MNCR policy to maintain records of inventory items using item numbers as identifiers, MNCR should include inventory at the Harmon Warehouse location in the PeopleSoft system using the proper identifiers.

***Management's Response:***

Metro-North agrees with this recommendation. The Maintenance of Way non-stock inventory for the Structures and Communication department located at Harmon is currently on spreadsheets. Metro-North will assign item numbers to this material and place the inventory into the PeopleSoft system by the end of the second quarter 2011.

**METRO-NORTH COMMUTER RAILROAD COMPANY  
CURRENT YEAR COMMENTS- 2009**

---

**2. PeopleSoft Database (Oracle)**

**A. Change Management**

***Observation:***

Currently, there is no centralized repository to maintain a list of changes made to the PeopleSoft database.

***Background:***

Per inquiry with the database administrator, it is noted that change control forms are utilized by his department but a centralized system for tracking these changes is currently not in place.

***Recommendation:***

Management should consider implementing a tracking system to maintain change control documentation for the PeopleSoft database. Such documentation should be centrally stored so that information can be easily retrieved when needed. Alternatively, management should consider using their existing repository for PeopleSoft changes (Request for Services Tracking Sheet) to also allow database documentation to be stored within that system.

***Management's Response:***

Metro-North agrees with this recommendation. We will evaluate the use of an electronic tracking system (RSTS or other system) by the fourth quarter 2010.

**B. Database Administration**

***Observation:***

A shared Database Administrator account (SYSADMIN) exists on the Oracle database. This account is used to make changes to the database.

***Background:***

The password to the shared SYSADMIN account is accessible by individuals on the database administration team. The SYSADM account is used because the team cannot assign these rights to their individual user accounts. A report showing a log of the host-names that access this account exists, but this report is only reviewed on a periodic basis.

***Recommendation:***

Management should consider reviewing the SYSADM host-name report on a regular basis. Any abnormal host-names accessing the account should be researched and investigated.

***Management's Response:***

Metro-North agrees with this recommendation. The recommendation was implemented in April 2010.

**METROPOLITAN SUBURBAN BUS AUTHORITY**

**METROPOLITAN SUBURBAN BUS AUTHORITY  
CURRENT YEAR COMMENTS- 2009**

---

**DEFICIENCIES**

We identified, and have included below, deficiencies involving the Metropolitan Suburban Bus Authority's (MSBA) internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention:

**1. Information Security- New User Access and User Access Reviews**

***Observation:***

New user access request forms were not available for three new hires selected for testing. Two of the users had access to Infor SmartStream application and one user had access to Vehicle and Asset Master Application.

In addition, user access reviews for Infor GL, Macola AP, Infor SmartStream, AFC, CISS Inventory Pro, and Vehicle and Asset Master Applications are performed informally. However, no documentation was provided evidencing such reviews.

***Background:***

We obtained a sample of the new users who were provided access to Infor SmartStream and Vehicle and Asset Master Applications. However, we were unable to obtain user access forms or other documentation supporting this process. We also noted that formal documentation relating to user access reviews is not retained.

***Recommendation:***

Documentation evidencing user access should be maintained in a central location. Management should also consider retaining evidence of periodic user access reviews within Infor GL, Macola AP, Infor Smartstream, AFC, CISS Inventory Pro, and Vehicle and Asset Master and other significant financial applications.

***Management Response:***

Procedures are being developed to document the workflow for application and or data access to include the requesting, approval, granting, reviewing and termination of user rights. Documentation for the access request will be completed with all steps recorded on the agency Business Application/Departmental Data Access Request Form IFTF002. The completed form will be electronically scanned to a dedicated folder and the paper form will be stored in a file at the Help Desk. Periodic user access reviews will be conducted and system users will be reviewed to verify their rights to the applications and data are based on current business needs.

**METROPOLITAN SUBURBAN BUS AUTHORITY  
CURRENT YEAR COMMENTS- 2009**

---

**2. Information Security- Password Controls**

***Observation:***

Password settings on the Infor GL application are not strong.

- No password complexity is enforced
- No password aging is enforced

***Background:***

The Infor GL application does not have strong password control that can help to protect the system.

***Recommendation:***

Management should consider implementing stronger password controls on the Infor GL application. Such controls can protect the system from unauthorized access as well as the maintenance of the data integrity.

***Management Response:***

Infor GL application is a legacy system that has minimal password controls. The vendor has indicated that there are no planned upgrades to the system to enhance or straighten password control. The Authority's intent is to replace the GL system with PeopleSoft's General Ledger which would be hosted and managed from MTA's Business Service Center. The migration to PeopleSoft will be completed by the first quarter 2011.

**MTA BUS COMPANY**

**MTA BUS COMPANY  
CURRENT YEAR COMMENTS- 2009**

---

**DEFICIENCIES**

We identified, and have included below, deficiencies involving the MTA Bus Company's ("MTA Bus" or the "Company") internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention:

**1. Inventory**

***Observations:***

1. Inventory adjustments were not always properly explained and/or supported by appropriate documentation.
2. Project work orders supporting labor hours and costs are not always entered into the Company's PeopleSoft system. Supporting documentation is not always available.
3. Inventory unit cost amounts are not always entered into the system.

***Background:***

Inventory Operations' personnel are responsible for the preparation and processing of all inventory adjustments. Storeroom personnel enter data for goods received and physical count adjustments and updated unit values. All transactions, including work order details are required to be entered into PeopleSoft.

***Recommendation:***

1. All inventory adjustments should be reviewed and approved before transactions are recorded into the PeopleSoft system. Adjustments should be prepared by Inventory Planning and reviewed by the Chief Material Officer or his/her designee. They should then be sent to the Controller's Department with proper support and documentation. The Controller's Department should then review and approve such. The Inventory Operations group should validate the adjustments entered into PeopleSoft to determine their accuracy and completeness.
2. All work orders should be entered into the system and appropriate supporting documentation maintained.
3. Storeroom personnel should not be permitted to process corrections. All adjustments should be assigned to a specific department and reviewed by management.

***Management Response:***

*Recommendation No. 1* - Agree. In late 2009, MTA Bus management requested MTA Audit Services to evaluate Internal Controls and processes relating to MTA Bus storeroom operations and related accounting impacts. Audit's independent assessment was sought to provide assistance in management's ongoing evaluation of existing procedures and development of new procedures. In conducting their assessment, Audit reviewed draft storeroom operation procedures, observed storeroom functions, reviewed various PeopleSoft and accounting reports, and performed limited testing of select practices. Audit's preliminary findings were issued in April 2010, and were generally consistent with those delineated in the

**MTA BUS COMPANY**  
**CURRENT YEAR COMMENTS- 2009**

---

**1. Inventory (continued)**

management report. Based on MTA Audit Service and the management report, MTA Bus is evaluating current and developing new procedures relating to storeroom and accounting functions and impacts.

These procedures will include requirements that; inventory adjustments are reviewed and approved before transactions are recorded into PeopleSoft, adjustments are prepared by Inventory Planning and reviewed by the Chief Material Officer or designee, adjustments are sent to the Controller's Department with proper support and documentation, and that the Controller's Department reviews and approves these adjustments. Additionally, the Inventory Operations group will be required to validate entries into PeopleSoft.

Recommendation No. 2 - Agree. Procedures referenced in recommendation no. 1 will also require that work orders are entered into the system and that documentation is retained.

Recommendation No. 3 - Agree. Procedures referenced in recommendation no. 1 will also identify the appropriate department to process and review storeroom corrections.

## **2. Interagency Transactions**

***Observations:***

Interagency inventory transfer billings between New York City Transit Authority (“NYCTA”) and MTA Bus are not always supported by appropriate documentation.

***Background:***

NYCTA and MTA Bus each maintain their own depots for the inventory of bus parts. When needed, parts are exchanged between Agencies for use in bus repairs. Interagency invoices are then prepared for billing.

***Recommendation:***

Documentation to support the exchange of bus parts should be provided with each interagency bill. Information should include date, depot location, part number, part description, quantity, unit cost and total value.

***Management Response:***

Agree. Procedures referenced in ‘Inventory’ recommendation no. 1 will also delineate the documentation required to be provided and retained for interagency transactions.

### **3. Information Security- PeopleSoft User Access Termination**

***Observation:***

One terminated user selected for testing continued to have an active PeopleSoft application account. The user was terminated from the agency on December 3, 2009.

***Background:***

We compared the terminated users with the list of all active application accounts in PeopleSoft. We noted that one terminated user continued to retain an active application account. According to Management, a request for deletion of the user's account was submitted in December, 2009 but was not processed.

***Recommendation:***

Management should consider disabling application accounts for terminated users in a timely manner. Request for deletion of access should be reviewed to make sure that the request has been completed. This will help to protect the system from unauthorized access.

***Management's Response:***

Monthly, MTA Bus will track and follow up on all Security requests that have been forwarded to supporting agency until completed.

## **1. Formal Written Documentation of the Various Internal Control Policies and Procedures**

### ***Observation:***

The MTA Bus needs to formally document all of the various internal control related policies and procedures which comprise their business operations.

### ***Background:***

The MTA Bus during the year ended December 31, 2007, went through several system migrations as it relates to the implementation of a general ledger system. During these migrations the MTA Bus worked diligently to ensure that the necessary controls relating to the initiation, processing and recording of the various transactions as well as the safe guarding of assets were in place. However, due to the laborious and ambitious time frame during which such implementation / conversion was occurring the necessary manual documentation of the various internal control policies and procedures for the business operations was not documented in a formal written manual. Such documentation is necessary to ensure that all employees of the MTA Bus Company adhere to and follow the internal control procedures developed by management to help mitigate and prevent fraud.

### ***Recommendation (2007):***

The MTA Bus needs to document formal written policies and procedures. Such documentation should be contained in a manual that details the various processes that need to be adhered to and followed by each employee in order to ensure that the necessary controls which management has implemented are functioning in the manner intended. This formal documentation will allow the MTA Bus Company to strengthen their controls and also act as a reference to employees on a go-forward basis.

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

The Controller's Office of MTA Bus concurs with the recommendations of the Deloitte & Touche auditors without reservation.

Written internal control policies and procedures were unavailable for review at the time of audit because investigation and identification of internal control deficiencies was actively underway, remediation procedures were being disseminated and current procedures were being recorded by the Subject Matter Expert (SME) for each system employed.

Policies and procedures have now been documented by SMEs. Formal, finalized manuals will be crafted to speak with one voice, with completion targeted for December 31, 2008. Such policies and procedures will address the internal control deficiencies identified as inherent to certain legacy systems by including the mitigating control(s) necessary to ensure financial statement integrity.

### ***Status Update (2008):***

This recommendation is considered partially completed as the MTA Bus is still in process of documenting formal written control policies and procedures.

### ***Management's Response (2008):***

During calendar year 2008, MTA Bus organizational structure was re-aligned to facilitate regional bus management with New York City Transit Bus ("NYC Transit Bus") and Long Island Bus. Operational and administrative policies have been, and continue to be, developed and issued to support a consistent regional management approach. MTA Bus continued to issue formal policies during 2008, and

**1. Formal Written Documentation of the Various Internal Control Policies and Procedures  
(continued)**

anticipates continued progress through 2009. This process is further supported by a more structured Internal Control program which is coordinated regionally for MTA Bus, NYC Transit Bus and Long Island Bus. Moreover, the Internal Control program is coordinated by the same unit which coordinates audits of MTA Bus, NYC Transit Bus and Long Island Bus.

***Status Update (2009):***

This recommendation is considered partially completed as the MTA Bus is still in process of documenting formal written control policies and procedures.

***Management Response (2009):***

MTA Bus continues to formalize policies and procedures and Internal Controls for all organizational areas. We have made strides in this area, as indicated in our comments concerning storeroom operations and accounting functions, management's evaluation and development of procedures is ongoing. While the evaluation of processes and procedures is an ongoing endeavor, we anticipate substantial completion by the completion of the next external audit cycle.

**NEW YORK CITY TRANSIT AUTHORITY**

**NEW YORK CITY TRANSIT AUTHORITY  
CURRENT YEAR COMMENTS- 2009**

---

**DEFICIENCIES**

We identified, and have included below, deficiencies involving the New York City Transit Authority's (NYCTA or Transit Authority) internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention:

**1. Communication Amongst Agencies**

***Observation:***

Information maintained by the Transit Authority regarding SIRTOA's pollution remediation outlays that did not qualify for capitalization was not provided to SIRTOA timely.

***Background:***

The Transit Authority maintains a workbook to identify its pollution remediation projects. This workbook contains SIRTOA's projects. In accordance with GASB Statement No. 49, such costs are required to be expensed. These projects were not communicated to SIRTOA and SIRTOA had initially capitalized these amounts erroneously as capital assets. Subsequent corrections were made and incorporated in SIRTOA's 2009 financial statements.

***Recommendation:***

Agencies' management should communicate data on each other's behalf on a timely basis.

***Management Response:***

Management concurs. Transit Authority and SIRTOA management have strengthened lines of communication regarding the timely notification and recording of pollution remediation expenditures and reserves.

***Target Date:***

Completed

## **1. Standardize Change Management Process across All Financially Significant Applications**

### ***Observation:***

Each financially significant application has a separate process for managing changes to the application. Testing previously identified the following points:

- For non-mainframe changes, there is no report from either a version control library or a production library to provide the system generated full population for all changes moved into production.
- Formal User Acceptance Testing and user sign-off were not consistently performed before the changes were submitted for migration into the production environment.
- There is no formal QA function to ensure the compliance of the process across all the applications, and a separate migration group has not been applied to all of the non-Mainframe applications.
- Manager approval was not consistently obtained before changes were migrated into the production environment.
- Evidence of IT testing was not always provided.
- There are segregation of duties issues in some applications where developers have access to both changing the code and promoting into production. In addition, while management restricted the sole developer's access to the production environment for the Remittance Recognition System (RRS) application, the developer also has access to the generic database administrator (DBA) ID, which has access to the production environment creating a segregation of duties conflict.

Based on management's original response and results of the 2008 audit procedures, this set of controls involves several major applications and implementation of corrective measures will be conducted in a phased manner. The remediation started in 2008 and is expected to be completed in 2009 and 2010 in stages. As such, this observation was determined to be in-process for the 2008 audit.

### ***Background:***

The lack of strong processes and controls to manage program changes to financially significant applications increases the risk that unauthorized changes are made to the application. In addition, lack of segregation of duties could result in unauthorized and inappropriate changes to the application. These risks may result in inadvertent program changes to applications that impact the processing of live business transactions, potentially affecting the integrity and accuracy of the financial statements.

### ***Recommendation (2008):***

Implement standardized processes and controls throughout New York City Transit for all changes that are made to applications that can have an effect on the financial statements (e.g., Automated Fare Collection AFC, Passenger Revenue Accounting System-PRAS, General Ledger-GIL, Kronos, Payroll, Employee Information System-EIS, Unified Timekeeping System-UTS, & Automated Timekeeping System-ATS). The following points should be considered in the controls:

- Use of standard request forms for both external (user group) & internal (Technology and Information Services-TIS group) requests.
- All requests should be tracked, monitored and approved appropriately by either the user group (for user requests) or by the respective TIS group manager.

**1. Standardize Change Management Process across All Financially Significant Applications  
(continued)**

- User testing, as well as programmer testing, should be implemented and documented for all changes and should include formal approval. In the case that user testing is deemed unnecessary, a formal waiver should be obtained and documented from the user group for each case.
- The responsibilities for developing the changes and moving the changes into the live production environment should be segregated (e.g., the people who code the changes should not have access to move changes to production and vice versa).
- A quality assurance function should be implemented to ensure that all of the requirements above are met prior to moving the changes to the production environment for all financial applications.
- Ensure appropriate segregation of duties exist for all application developers; restrict developer's access to the production environment. If segregation of duties is not possible consider implementing a monitoring control whereby program changes are monitored by a resource independent of application developers to validate that the program change controls are not circumvented.

***Management Response (2008):***

Management concurs. Standardization of the Change Management/QA functions across all financially significant applications is ongoing. Because this process involves several major applications, implementation will be conducted in a phased manner and is expected to be completed in 2010.

***Target Dates:***

Phase II: Process implementation for limited critical applications — Implemented

Phase III: Review results and develop a roll out plan for all financially significant applications — Implemented.

Phase IV: Deploy to remaining financially significant applications — 4th quarter, 2010.

***Status Update (2009):***

Management is in the process of implementing a standard change management request form system across all financially significant applications.

This issue has not been addressed is still open.

***Management Response (2009):***

We are on schedule as outlined in the 2008 Management Response and continue to move forward to include all the financially significant applications not scheduled to be transferred to the Business Service Center (BSC).

***Target Date:***

Phase IV: Deploy to remaining financially significant applications - 4th Quarter 2010.

**NEW YORK CITY TRANSIT AUTHORITY  
PRIOR YEAR COMMENTS- 2008**

---

**2. Enhance (1) User Access Provisioning Procedures and (2) User Access Removal Procedures for Terminated Employees**

***Observation:***

(1) Management has implemented new user provisioning policies and procedures for the Automated Timekeeping System (ATS) and Kronos. However, previous testing of the user access provisioning identified that users were not consistently approved prior to the creation of the user ID over the applications.

(2) Our review of user terminations hosted that some users still had access to financially significant systems even though they had been terminated. This included 35 terminated users who retained access to the Unified Timekeeping System (UTS), and 27 terminated users who retained access to the Novell Local Area Network.

Based on management's original response and results of the 2008 audit procedures, remediation of the observations above started in 2008 and is expected to be completed in 2009 based on migration to I- Vault and the roll-out of the ATS security software. As such, this observation was determined to be in- process for the 2008 audit.

***Background:***

(1) Deviation from procedure and controls for setting up user access increases the risk of unauthorized and/or inappropriate access to financially significant applications, and may compromise the integrity of the data for such applications.

(2) If termination procedures are not consistently applied, there is an increased risk of unauthorized access to the financial systems when user accounts for employees who no longer work for New York City Transit are still enabled.

***Recommendation (2008):***

(1) Reinforce compliance over granting user access to ensure that users are given access only upon proper approval and based on job responsibility.

(2) Consistently follow the processes to revoke/disable the access of all terminated employees in a timely manner from all financially significant applications.

***Management Response (2008):***

Automated Timekeeping System (ATS): Management concurs. Rollout of the new procedures requires coordination and synchronization of effort on the part of both Technology and Information Services (TIS) and ATS customer security liaisons. Given that the pace of rollout cannot be set by TIS alone, the rollout is proceeding at a slower pace than originally anticipated.

Kronos/Unified Timekeeping System (UTS): Management Concurr. In April 2008, the I-Vault interface with Kronos was implemented. I-Vault updates Kronos with demographic data from the

**NEW YORK CITY TRANSIT AUTHORITY  
PRIOR YEAR COMMENTS- 2008**

---

**2. Enhance (1) User Access Provisioning Procedures and (2) User Access Removal Procedures for Terminated Employees (continued)**

Employee Information System (EIS). Based on this information, Kronos access is updated. Eventually access to all systems, including UTS, will be controlled by I-Vault. This will insure standard accessing procedures for all systems.

***Target Dates:***

ATS: 2nd quarter 2009 through 1st quarter 2010.

Kronos: Partially implemented. Implementation of a standard access protocol (LDAP) interface scheduled for the 2nd quarter of 2009 will address the remaining findings.

UTS 4<sup>th</sup> quarter 2009 through 1st quarter 2010.

***Status Update (2009):***

5 out of 25 terminated users selected for testing continued to have active application IDs. This included users who retained access to the GL System, ATS, UTS and EIS applications. However, it was noted that their network and physical access was removed.

Further it was noted that I -Vault interface for Kronos has been successfully implemented. This implementation is still in process for UTS. For ATS, the rollout of I-Vault is still in its planning stages.

This issue is still open.

***Management Response (2009):***

Automated Timekeeping System (ATS): The new ATS security module was developed and completed in 2009 by ATS Applications to address this and other audit recommendations. The ongoing rollout of the attendant new security procedures continues to require coordination and synchronization of effort on the part of both Technology and Information Services (TIS) Security and ATS Customer Security Liaisons. ATS management will continue to make every effort to enlist maximum customer cooperation on this joint effort going forward.

Kronos – Implemented. In June 2009, LDAP connectivity for the KRONOS Workforce Central (WFC) Timekeeping System was implemented. As a result, all employees who use WFC must now access this system through MYACCESS. WFC is now following what will eventually be the universal standard for New York City Transit Authority in terms of user access provisioning procedures, user access removal procedures, periodic reviews over access controls, and password controls. WFC no longer controls any of these functions. LDAP connectivity using MYACCESS controls all these functions and provides a secure access environment.

**NEW YORK CITY TRANSIT AUTHORITY  
PRIOR YEAR COMMENTS- 2008**

---

**2. Enhance (1) User Access Provisioning Procedures and (2) User Access Removal Procedures for Terminated Employees (continued)**

UTS - First phase of I-Vault implementation - Database upgrade from 9i to 10g completed in April 2010. The second phase, the implementation of LDAP for the I-Vault interface, is in development and scheduled to be completed by the 4th quarter of 2010.

General Ledger: The Controller's Office has the ability to remove access to the system on an individual basis. Given this system will be moving to the BSC in January 2011, there are no plans to connect it to I-Vault.

One of the employees noted was a training liaison for his depot. He had access to Training modules in EIS and logon to EIS with an individual user profile. This user profile was not connected to I-Vault because the Training module of EIS is not managed by I-Vault. He utilized only EIS training module which TIS Security set up for him in PeopleSoft.

TIS Security will run a manual report on a daily basis to capture all separated employees.

Currently only Kronos has full connector. Not all other systems are on schedule for I-Vault connection yet, and due to the current budgetary situation and lack of available recourses, we estimate completion by 1<sup>st</sup> Quarter 2012.

***Target Dates:***

ATS: 4<sup>th</sup> quarter 2010.

LDAP: 4<sup>th</sup> quarter 2010.

UTS: 1<sup>st</sup> quarter 2012.

### **3. Expand Periodic Reviews Over Access Controls**

***Observation:***

For the Automated Timekeeping System (ATS), Kronos and the Unified Timekeeping System (UTS), there are no periodic reviews of operating system security parameters, to ensure they remain appropriate and adequate over time. Also, there is no evidence that periodic reviews of user access are performed for ATS, Kronos and UTS.

Based on management's original response and results of the 2008 audit procedures<sup>1</sup> remediation of the observations above started in 2008 and is expected to be completed in 2009 based on migration to I-Vault, migration to a newer version of UTS and the roll-out of the ATS security software. As such this observation was determined to be in-process for the 2008 audit.

***Background:***

The lack of periodic reviews of system security parameters and users increases the risk that unauthorized and inappropriate changes to system parameters and user accounts may go undetected and uncorrected over time.

***Recommendation (2008):***

Perform periodic reviews throughout the year for all financially significant applications and system environments to ensure that all system security parameters and employee access rights are appropriate and adequate overtime.

***Management Response (2008):***

Automated Timekeeping System (ATS): Management concurs. These periodic reviews will be formalized as one material component of the comprehensive new security procedures currently being developed.

Kronos: Management Concurs. Currently Kronos is in the process of implementing a standard access protocol (LDAP) with the I-Vault to Kronos interface. Once this is completed, I-Vault will control access to Kronos. Continuous review of I-Vault and its parameters will validate access control.

Unified Timekeeping System (UTS): Management concurs. This is an area that is completely controlled by the local depot managers. UTS Applications' only involvement is a report supplied by Technology and Information Services (TIS) to assist users in performing periodic reviews: Implementation of the I-Vault to UTS interface will address these access controls.

***Target Dates:***

ATS: 2nd quarter 2009 through 1st quarter 2010.

Kronos: Implementation of LDAP for the I-Vault interface is scheduled to be completed by 2nd quarter 2009.

UTS: Based upon implementation of the vault Interface with UTS — 4th quarter 2009 thru 1st quarter 2010.

**NEW YORK CITY TRANSIT AUTHORITY  
PRIOR YEAR COMMENTS- 2008**

---

**3. Expand Periodic Reviews Over Access Controls (continued)**

***Status Update (2009):***

No periodic access recertification is currently being performed for the users with access to UTS application.

This issue is still open.

***Management Response (2009):***

Automated Timekeeping System (ATS): These periodic reviews are one material component of the comprehensive new security procedures completed in 2009 and currently being rolled out by TIS Security. Implementation is scheduled for 4th quarter 2010.

Kronos – Implemented. In June of 2009 LDAP connectivity for the KRONOS Workforce Central (WFC) Timekeeping System was implemented. As a result, all employees who use WFC must now access this system through MYACCESS.

UTS - Application security is locally managed by depots and subdivision management. Implementation of I-Vault will prevent unauthorized access to the system. Status - First phase of I-Vault implementation - database upgrade from 9i to 10g - completed in April 2010. Implementation of the second phase is in development and scheduled for completion by the 1st quarter of 2012.

***Target Dates:***

ATS: 4th quarter 2010.

Kronos: Implemented.

UTS: 1st quarter 2012.

#### **4. Strengthen password controls for ATS, Kronos and UTS**

***Observation:***

There are various weaknesses in password parameters in the following application environments: the Automated Timekeeping System (ATS), Kronos and the Unified Timekeeping System (UTS). Examples of these are as follows:

- Passwords do not expire.
- Password complexity is not enabled.
- No account lockout.
- No password minimum length.

Based on management's original response and results of the 2008 audit procedures, remediation of the observations above started in 2008 and is expected to be completed in 2009 based on migration to I-Vault, migration to a newer version of UTS and the roll-out of the ATS security software. As such, this observation was determined to be in-process for the 2008 audit.

***Background:***

If strong password controls (e.g., password expiration, minimum length, etc.) are not enabled for all financially significant applications, there is an increased risk of unauthorized access.

***Recommendation (2008):***

Consider the following options by applying a risk based approach for each application:

- Strengthen password controls over the specific applications and systems listed above to enforce complex password configurations.
- If password controls cannot be changed due to inherent risks caused by system limitations, implement compensating controls (such as monitoring of certain transactions) to mitigate the risk of unauthorized access to systems.

***Management Response (2008):***

Automated Timekeeping System (ATS): Management concurs. Strengthened password controls are an intrinsic material component of the comprehensive new security procedures mentioned in the previous user access provisioning procedures and controls findings.

Kronos: Management concurs. Currently Kronos is in the process of implementing an access protocol with the I-Vault to Kronos Interface, once this is completed, password expiration, password complexity; account lockout and minimum password length will be controlled by the I-Vault System. Eventually, access to all systems will be controlled by I-Vault. Therefore, there will be standard password controls for all systems.

Unified Timekeeping System (UTS): Management concurs. The Departments of Buses and Rapid Transit Operations user groups have full control over access to the database. The current UTS database version in use does not provide sufficient login or password expiration controls. However; implementation of the I-Vault to UTS interface will expire passwords after 30 days and whenever employees become inactive. This will have the effect of locking out old accounts and enforcing adequate password controls.

**NEW YORK CITY TRANSIT AUTHORITY  
PRIOR YEAR COMMENTS- 2008**

---

**4. Strengthen password controls for ATS, Kronos and UTS (continued)**

***Target Dates:***

ATS: 2nd quarter 2009 through 1st quarter 2010.

Kronos: Implementation of LDAP for the I-Vault interface is scheduled to be completed by 2nd quarter 2009.

UTS: 4th quarter 2009 through 1st quarter 2010.

***Status Update (2009):***

There are password weaknesses in the password controls for ATS, UTS and the Fixed Assets Control System.

Examples of these are as follows:

- Passwords do not expire
- Password complexity is not enforced
- No account lockout after invalid login attempts

This issue has is still open.

***Management Response (2009):***

Automated Timekeeping System (ATS): Strengthened password controls are an intrinsic material component of the comprehensive new security procedures completed in 2009 and currently being rolled out by TIS Security. Implementation is scheduled for 4th quarter 2010.

Kronos – Implemented.

UTS – The first phase of I-vault implementation - database upgrade from 9i to 10g - completed in April 2010. Implementation of I-Vault access protocol is in development and scheduled to be completed by the 4th quarter of 2010. Once completed, I-Vault will control password expiration, password complexity, account lockout and strengthen existing minimum password length.

The standard NYCT password policies are applied to all systems and applications connected to I-Vault. Those systems that are not connected do not have centralized password management and password policies; their password maintenance is the internal procedure of system (application) owners and their support teams. The connection of those systems to I-Vault even via simple LDAP interface can address this issue and correct the problem.

***Target Dates:***

ATS: 4th Quarter 2010.

UTS: 4th Quarter 2010.

**STATEN ISLAND RAPID TRANSIT OPERATING AUTHORITY**

**STATEN ISLAND RAPID TRANSIT OPERATING AUTHORITY  
CURRENT YEAR COMMENTS- 2009**

---

**DEFICIENCIES**

We identified, and have included below, deficiencies involving the Staten Island Rapid Transit Operating Authority's ("SIRTOA") internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention:

**1. Workers' Compensation Underlying Data**

***Observation:***

The actuarial analysis prepared by Milliman to calculate the estimated workers' compensation liability arising from injuries to persons did not include the entire population of claim payments made during the year. We noted that in five of the files selected for testing there was evidence that SIRTOA made medical payments. Such payments were not reflected in data used by Milliman. The file provided to them indicated a zero amount.

***Background:***

Cases are processed by the Transit Authority using the workers compensation information system ("WCIS"). The Transit Authority approves the payments and then they are disbursed through SIRTOA's operating cash account.

The problem with some payments is caused by the upload process from WCIS to the risk management information system ("RMIS"). RMIS is the system used to collect the data to send to Milliman. RMIS captures the payments by using the check date field. If the check date field is not populated, RMIS does not note the payment. Since the medical payments are paid by SIRTOA, the check date field is not populated by the Transit Authority management in the WCIS, thus the medical payment information is not transferred to the RMIS system and not captured in the underlying data used by Milliman. The 2009 files were subsequently resent to Milliman with the entire population of payments included. Such data was incorporated into the current calculation.

***Recommendation:***

Management should enter into the WCIS system the date that the medical claim check was disbursed by SIRTOA. Once downloaded to RMIS, the file for the claims payments will be complete for use by Milliman.

***Management's Response:***

Management concurs with this recommendation. SIRTOA, NYCTA and MTA Risk Management have taken the necessary steps to ensure that workers compensation payments made by SIRTOA are properly captured and recorded in the NYCTA WCIS and MTA RMIS systems and accurately reported for actuarial valuation.

**STATEN ISLAND RAPID TRANSIT OPERATING AUTHORITY  
CURRENT YEAR COMMENTS- 2009**

---

**2. Communication Amongst Agencies**

***Observation:***

Information maintained by the Transit Authority regarding SIRTOA's pollution remediation outlays that did not qualify for capitalization was not provided to SIRTOA timely.

***Background:***

The Transit Authority maintains a workbook to identify its pollution remediation projects. This workbook contains SIRTOA's projects. In accordance with GASB Statement No. 49, such costs are required to be expensed. These projects were not communicated to SIRTOA. Total expenditures in FY 2009 amounted to \$534,830 and the total accrual at December 31, 2009 was \$286,799. SIRTOA had initially capitalized these amounts erroneously as capital assets. Subsequent corrections were made and incorporated in SIRTOA's 2009 financial statements.

***Recommendation:***

Agencies' management should communicate data on each other's behalf on a timely basis.

***Management's Response:***

Management concurs with this recommendation. SIRTOA and NYCTA management have strengthened lines of communication regarding the timely notification and recording of pollution remediation expenditures and reserves.

**TRIBOROUGH BRIDGE AND TUNNEL AUTHORITY**

**TRIBOROUGH BRIDGE AND TUNNEL AUTHORITY  
CURRENT YEAR COMMENTS- 2009**

---

**DEFICIENCIES**

We identified, and have included below, deficiencies involving the Triborough Bridge and Tunnel Authority's (TBTA) internal control over financial reporting as of December 31, 2009, that we wish to bring to your attention:

**1. Casual Use (E-ZPass) Receivables**

***Observation:***

E-ZPass receivables were not updated as of December 31, 2009 for adjustments received in January 2010 related to December 2009.

***Background:***

E-ZPass adjustments related to the month of December are not finalized until the settlement is received in the subsequent month. The difference represented transactions that transpired during 2009, and should therefore have been recorded as part of December 31, 2009 receivables. The amounts are known upon settlement of casual use payables and receivables subsequent to December 31, 2009 but prior to closing the books.

***Recommendation:***

Management should record all E-ZPass adjustments in the correct accounting period.

***Management's Response:***

Management agrees to record all E-ZPass adjustments (that relate to the prior year) that are settled in January, prior to the completion of the Surplus Calculation on or about February 1st.

**TRIBOROUGH BRIDGE AND TUNNEL AUTHORITY  
CURRENT YEAR COMMENTS- 2009**

---

**2. Unamortized Bond Premium**

***Observation:***

Unamortized bond premium related to TBTA General Revenue Bonds, Series 2008C was not amortized on a quarterly basis.

***Background:***

Through the examination of the Q1 and Q2 journal entries, it was noted that the unamortized bond premium related to TBTA General Revenue Bonds, Series 2008C was not amortized in either of the first two quarters of 2009. The missed amortization will be distributed throughout the 4 quarters of 2010, such that by the end of 2010, the balance of unamortized premium for TBTA General Revenue Bonds, Series 2008C will be corrected.

***Recommendation:***

Management should review the calculation of unamortized bond premium on a quarterly basis to ensure all necessary entries have been recorded in the proper accounting period. This review should be evidenced by management signoff.

***Management's Response:***

We agree with the comment on Unamortized Bond Premium and will implement additional procedures to have management review and sign-off on premium amortization calculations on a quarterly basis.

**TRIBOROUGH BRIDGE AND TUNNEL AUTHORITY  
CURRENT YEAR COMMENTS- 2009**

---

**3. Information Security- Macola Application User Access**

***Observation:***

One Macola application user account was still active within the application; however the account was no longer required by the account owner and should have been disabled.

***Background:***

It was noted that one user left TBTA employment on December 2, 2009, but was still listed as an active user in the Macola User listing as of January 22, 2010.

***Recommendation:***

Management should disable the application account belonging to the terminated user. In addition, management should also consider enforcing timely notification to the IT department to immediately remove user access to the network and applications for all terminated users.

***Management's Response:***

Management agrees with the recommendation. Pending the request coming from the Procurement Department, the Technology Department initially disabled the user account from the Network on December 7, 2009. The request from the User Department came on February 10, 2010 and the Technology Department then disabled the user from Macola as well.

**TRIBOROUGH BRIDGE AND TUNNEL AUTHORITY  
PRIOR YEAR COMMENTS- 2006**

---

**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.

***Recommendation (2006):***

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 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, the TD, in conjunction with the Finance Department, will re-visit and re-evaluate the issue and decide whether this can be done in 2008.

***Status Update (2008):***

The Macola application upgrade is currently on hold. Hence, the Controller's Department will be instituting additional manual controls over Macola processing which will be in effect by April 30, 2009.

Management is addressing this item. This comment is still open.

***Management's Response (2008):***

The Controller's Department will be instituting additional manual controls over Macola processing which will be in effect by April 30, 2009.

**TRIBOROUGH BRIDGE AND TUNNEL AUTHORITY  
PRIOR YEAR COMMENTS- 2006**

---

**1. Information Security (continued)**

***Status Update (2009):***

The Macola application upgrade is still on hold. The upgrade is currently scheduled for early 2011.

Management is addressing this item. This comment is still open.

***Management's Response (2009):***

The Macola application upgrade is now out of scope due to the PeopleSoft Enterprise Resource Planning implementation at the Business Service Center. The new finance system is scheduled to go live in early 2011. However, the Controller's Department will continue its manual controls over Macola processing until the new system is fully implemented.

**PRIOR YEAR COMMENTS ADDRESSED**

## **PRIOR YEAR COMMENTS ADDRESSED**

---

### **Metropolitan Transportation Authority- Headquarters**

1. Novell Netware Security- 2008
2. No Review of Subsequent Disbursements Performed During the Closing Period- 2007
3. Aged Request for Proposal (“RFP”) Deposits Payable- 2006

### **First Mutual Transportation Assurance Company**

1. Writing Insurance Policies- 2008
2. Review of Unearned Revenue- 2008

### **Long Island Rail Road Company**

1. RSMS Application Security- 2008
  - a) Password Configuration
  - b) Backup Logs
1. GEAC Application Security- 2008
2. CSS Application Security- 2008
3. UNIX (RSMS) Security- 2008
4. Novell (Network) Security- 2008
  - a) Intruder Detection Settings
  - b) Novell User Access

### **Metro-North Commuter Railroad Company**

1. PeopleSoft Financial Application Security- 2008
2. Network (Windows) Security- 2008
3. PeopleSoft Financial Application Security- 2008

### **Metropolitan Suburban Bus Authority**

None

## **PRIOR YEAR COMMENTS ADDRESSED**

---

### **MTA Bus Company**

1. VAX Application Security- Backup Tapes- 2008
2. VAX Application Security- Segregation of Duties- 2008
3. VAX Application Security- User Access Review- 2008

### **New York City Transit Authority**

None

### **Staten Island Rapid Transit Operating Authority**

None

### **Triborough Bridge and Tunnel Authority**

1. Revenue Accounts Netted Against Expense Accounts- 2008
2. Information Security- Windows 2000 Security- 2008
3. Information Security- PeopleSoft User Access Revalidation- 2008
4. Information Security- PeopleSoft Segregation of Duties- 2008
5. Change Management- PeopleSoft Change Control- 2008
6. Management Review of the Accounts Receivable Reserve- 2008
7. UNIX and RAAS Application Security- 2007

## **APPENDIX B**

## **DEFINITION**

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

A *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 and correct 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 would not be met. A deficiency in operation exists when (a) a properly designed control does not operate as designed, or (b) the person performing the control does not possess the necessary authority or competence to perform the control effectively.

\* \* \* \* \*