The Metropolitan Transportation Authority

Report to Management

Year Ended December 31, 2011
May 2, 2012

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, 2011 (on which we have issued our reports dated May 2, 2012 with the exception of the New York City Transit Authority and Staten Island Rapid Transit Operating Authority.), 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, 2011, that we wish to bring to your attention.

We have also issued a separate report to the Audit Committee, dated April 25, 2012, which included a certain matter involving the Staten Island Rapid Transit Operating Authority’s internal control over financial reporting that we consider to be a material weakness under standards established by the American Institute of Certified Public Accountants.

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,

[Signature]
# THE METROPOLITAN TRANSPORTATION AUTHORITY

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A</td>
<td></td>
</tr>
<tr>
<td>Metropolitan Transportation Authority- Headquarters</td>
<td>6</td>
</tr>
<tr>
<td>MTA Business Service Center</td>
<td>19</td>
</tr>
<tr>
<td>Long Island Rail Road Company</td>
<td>41</td>
</tr>
<tr>
<td>Metro-North Commuter Railroad Company</td>
<td>47</td>
</tr>
<tr>
<td>MTA Bus Company</td>
<td>52</td>
</tr>
<tr>
<td>New York City Transit Authority</td>
<td>56</td>
</tr>
<tr>
<td>Triborough Bridge and Tunnel Authority</td>
<td>63</td>
</tr>
<tr>
<td>Prior Year Comments Addressed</td>
<td>71</td>
</tr>
<tr>
<td>Appendix B</td>
<td></td>
</tr>
<tr>
<td>Deficiency Definition</td>
<td>74</td>
</tr>
</tbody>
</table>
METROPOLITAN TRANSPORTATION AUTHORITY - HEADQUARTERS
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, 2011, that we wish to bring to your attention:

1. Succession Planning

Observation:
This comment has been tailored for the MTAHQ Accounting Department from the best practices issued by the Government Finance Officers Association (“GFOA”), as we feel it is applicable.

Many governments face the challenge of ensuring continuity and consistency of service delivery due to employee turnover. In instances where large numbers of government employees are eligible to retire, there is a concern that not enough qualified or available workers will be prepared to replace them.

Background:
The GFOA encourages governments to address the following key issues and develop strategies concerning succession planning.

- Develop an integrated approach to succession management. Organizations with an integrated, rather than “just-in-time,” approach to succession management experience higher retention rates, increased employee morale, and an environment that stimulates innovation and organizational change. There are some positions in an organization that are more critical than others. A successful succession plan should place a high priority on planning for a smooth change in such positions. Key components of an integrated succession management approach include: workforce planning, succession planning, knowledge management practices, and recruitment and retention practices.

- Continually assess potential employee turnover. Making career planning discussions a part of a regular and ongoing performance review process assists in assessing potential turnover. Department heads are a good resource in helping to identify employees that may be planning to leave.

- Provide a formal, written succession plan as a framework for succession initiatives. Without a formal plan, workforce/succession planning tends to take place in a haphazard fashion. A formal plan identifies risks and strategies, thereby providing a guiding framework for specific succession initiatives, including how employees are eligible to participate and what being part of the succession plan means. Plans that have been thoughtfully articulated and communicated to the organization are more likely to be successful. Additionally, having a formal plan indicates organization and leadership commitment to succession management, which is critical for success and for sustaining successful planning across political and leadership transitions. The Budget Department and the Human Resources Department should work together to develop this plan, along with other departments as needed.

- Develop written policies and procedures to facilitate knowledge transfer. Knowledge transfer is a critical component of succession management. There should be written procedures in place to
1. Succession Planning (continued)

- formalize the knowledge transfer. A meeting should be held with departing staff to document job responsibilities.

- Development of leadership skills should be a key component of any succession planning initiative. When leadership development occurs, the organization benefits from developing a leadership pool for other positions.

- Encouragement of personal professional development activities should be a key part of the succession planning effort. Personal professional development benefits the organization over the long term by helping employees gain the skills they need to assume increased responsibilities.

- Design of better recruitment and retention practices may aid in the succession process. Many organizations will focus more on recruiting the new employee and less on orienting the person to the position and the ongoing development of the employee. Making sure pay levels are competitive with the market place is one means of retaining employees. Providing career advancement opportunities for employees is another means of retention.

- Consideration must be given to collective bargaining agreements and how those agreements fit in with the overall succession plan. The engagement of bargaining units for cross training opportunities is encouraged.

- If early retirement programs are offered by your entity, it should be done in conjunction with a succession plan. GFOA strongly recommends that governments use considerable caution when considering the implementation of early retirement plans (see GFOA’s Advisory: Evaluating the Use of Early Retirement Incentives). If an early retirement program is offered, that might provide a window of opportunity to look at technology, potential to streamline, or rethinking the way services are provided, managed, and/or administered.

- Consider non-traditional hiring strategies. Options such as part-time work, job-sharing, volunteers, and flexible schedules and flexible-place arrangements are providing mechanisms to both meet the needs of the organization and employees.

References:


Approved by the GFOA’s Executive Board, February, 2011.

Recommendation:
It is recommended that the MTAHQ Accounting Department implement a strategic approach to succession planning at all levels, including the identification of mission critical positions and succession pools; workforce analytics to identify potential high loss separations from the MTAHQ Accounting
1. Succession Planning (continued)

Management; leadership development programs focused on continuous development and retention of high potential employees; and external recruitment for new staff who can grow and adapt to future MTAHQ Accounting Department needs.

Management Response:
We agree with this recommendation. Recently, steps have been taken to implement succession plans for key critical positions in the HQ Comptroller’s Department. High potential current employees have been identified and are being retained and developed to replace the future retirements of the Deputy Comptroller for Revenue and Capital Disbursements as well as the Deputy Comptroller for General Accounting. We will be reviewing key positions at all levels for succession candidates and will identify programs for development and cross-training so that identified employees gain the skills they need to assume increased responsibilities.
2. Underlying Data Sent to the Actuary

Observation:
The underlying payroll information, which was used to calculate the December 31, 2011 Other Postemployment Benefits liability (“OPEB” or “GASB 45”), provided by MTAHQ to the actuary did not contain the correct salary information.

Background:
The MTA uses a third party actuarial firm to calculate the OPEB liability on a biennial basis. The actuarial firm relies on MTAHQ management to provide complete and accurate underlying data records such as headcount totals and salary information. The actuarial firm uses this information to calculate the resulting OPEB liability.

It was noted that the salary information MTAHQ provided to the actuarial firm for the December 31, 2011 OPEB liability calculation contained incorrect salary information. The salary information provided to the actuarial firm should have represented the compensation rate as of January 1, 2010. However, differences existed between the compensation rate per the PeopleSoft system and the data submitted to the actuary. Through additional inquiry, it was determined that during the transition of the MTAHQ payroll function to the MTA BSC in early 2011, there was an error in gathering the payroll data that was sent to actuarial firm which resulted in an understatement of the December 31, 2011 OPEB liability in the amount of $1.77 million.

Recommendation:
It is recommended that MTAHQ perform review procedures on the underlying salary information prior to sending such information to the actuarial firm.

Management Response:
We agree with the finding and will implement the recommendation this year.
3. Consistent Reports

Observation:
Reports that are provided to the Board of Directors, Finance Committees, and Audit Committees are not consistent and do not report the same financial information.

Background:
The MTA and its agencies report monthly to various boards and committees including Boards of Directors, Finance Committees, and Audit Committees. The current financial positions of the MTA and its agencies are presented at these meetings in the form of monthly or quarterly financial statements. However, due to the timing of these meetings, the financial information presented to one committee could differ from the financial information presented to another committee. For instance, closing accrual entries may have not been recorded in the financial information presented to the Finance Committee, however were included in the financial information presented to the Audit Committee.

Recommendation:
All financial information presented to the Boards of Directors, Finance Committees, and Audit Committees should be the same and include all closing entries needed to present the financial information in accordance with GAAP.

Management Response:
MTA monthly financial reporting is designed to provide up-to-date information to the Board, the public and elected officials on a monthly basis. Information is segregated by Agency so that each Board Committee has the most accurate, current and useful information. This construct results in a few discrepancies when compared with the quarterly consolidated numbers that are reviewed by our auditors. These discrepancies are identified and quantified and do not result in any material misrepresentation of MTA’s financial performance. The current construct allows for the most cost-effective and timely method of measuring financial performance while the quarterly and annual audit process ensures compliance with GAAP accounting rules.

The Audit Committee typically reviews the audited consolidated financial results in the April meeting following the fiscal year end. The audited consolidated financial statements include supplemental schedules which provide reconciliations between the audited consolidated statement of Revenues, Expenses and Changes in Net Assets and the Financial Plan estimated fiscal year actual results. For Fiscal Year 2011, the total net variance between the estimated Financial Plan and the audited results was $117.4 million. Most of this variance ($108 million) is attributable to the New York State subsidy for debt service which is netted in debt service payments in the Financial Plan. In the July Finance Committee meeting, the final prior year results are presented with the current year estimated actuals and next year’s preliminary budget.

*Observation:*
It was noted that there are no audit logs being generated to capture security events (e.g. security violations, monitoring the use of the system, etc.) at the Impact application level.

*Background:*
As part of our assessment for the Impact application, we noted through discussions with management, there is currently no procedure in place to generate and review security logs on a regular basis.

*Recommendation:*
Management should consider generating and reviewing audit logs for critical applications in order to detect certain security events within the system. These audit logs should be generated and reviewed at fixed intervals determined by management. Evidence of such review should be retained so that it can be made available upon request.

*Management’s Response:*
In April 2012, the MTA began leveraging logging features to capture security events within Impact with a middleware application server. This capability logged successful and failed login attempts. Because the middleware application authorizes all users stored in an associated LDAP database, audit logs are generated.

Additionally, procedures have been developed to regularly review these audit logs for anomalous activity and document the related findings.
5. User Access Reviews- IMPACT Application

Observation:
User access reviews for the IMPACT application are performed informally. No documentation evidencing the user access review could be obtained.

Background:
It was noted that formal documentation relating to user access review for the Impact application is not retained. Per discussion with management, we noted that the reviews were performed; however, no documentation was available to evidence the review.

Recommendation:
Management should consider documenting evidence for the user access reviews for Impact. This documentation should be retained so that it can be made available when needed. The documentation should include details of the review such as date of review, names of personnel whose access is reviewed and sign offs by the manager(s) performing the review.

Management’s Response:
A recertification initiative of IMPACT users is scheduled for Summer 2012. Additionally, existing procedures around account management will be embellished to incorporate activities that will document user additions, changes and terminations.
6. Change Management- Impact Application

Observation:
A change tracking tool was not used in 2011 to track changes to the Impact application. A manual list showing all the changes to the application was also not maintained.

Background:
It was noted the MTA used the Team Track product to document issues and subsequent changes that were needed to be made to the Impact application. During 2011, however, the application was no longer available and a manual process was implemented to bridge the gap until a new system was deployed. As a result, we were unable to obtain formal documentation showing the list of all the changes that took place within Impact.

Recommendation:
Management should maintain a tool or tracking system to track all the changes to the application. This will help to establish a central repository for the changes and prevent unauthorized changes from being made to the application.

Management’s Response:
In early 2012, the MTA replaced the decommissioned Team Track application with Redmine, which is a flexible, project management tool with change tracking features.
1. 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 (2009):*
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.

*Status Update (2010):*
It was noted that the MTA paid back $500 million from the Transportation Capital Project Non Bond Proceed account to the General Fund Account in the amount of $400 million and the NYCTA Stabilization Account in the amount of $100 million on December 30, 2010. However, MTA reloaned $500 million from the same sources to the Transportation Capital Project Non-Bond Proceed account on December 30, 2010. As of December 31, 2010, the $500 million was still outstanding.

*Management Response (2010):*
The MTA Consolidated 2011-2014 Financial Plan anticipates repaying this loan in 5 annual installments beginning in 2012.

*Status Update (2011):*
As of December 31, 2011, the $500 million was still an outstanding loan.

*Management Response (2011):*
As per MTA’s Financial Plan and as required by the loan document we are scheduled to repay the entire $500 million at end of 2012 and re-issue a $400 million loan. Therefore, this $500 million loan is scheduled to be repaid in five (5) annual installments of $100 million starting December 2012.
2. 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 (2009):*  
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.

*Status Update (2010):*  
This issue has not been resolved. We reiterate our comment from prior year and this issue is still open.

*Management Response (2010):*  
Though the procedure described above to reconcile Federal grants requisitioned to the total reported in the general ledger and the financial statements has been implemented in 2010 and is currently monitored, the identified variances have not yet been corrected. These variances will be resolved in 2011.

*Status Update (2011):*  
This issue has not been resolved. We reiterate our comment from prior year and this issue is still open.

*Management Response (2011):*  
The Revenue and Accounting departments have accomplished elimination of variances when it comes to setting up the Template for the General Ledger. The present process entails the Revenue department approving the set-up of the debits and credits in the PeopleSoft General Ledger for each new funding by maintaining a look up table in the IMPACT system.

To further ensure agreement of fund balances reported in the consolidated financials, Accounting will acquire Revenue Department approval for any related manual journal entries in PeopleSoft G/L. This would ensure that the amount and the source of funding is correctly identified.
3. 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 predetermined 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 (2009):
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.

Status Update (2010):
No action was taken in 2010 with respect to implementation of any of the above mentioned solutions.

Management’s Response (2010):
A recent upgrade has allowed us to enforce password length requirements; however, the technology is still unable to address password aging or password history. These additional recommendations will be implemented as soon as our software platform (Weblogic) allows it.
3. Impact Application Password Configuration (continued)

**Status Update (2011):**
No action was taken in 2011 with respect to implementation of any of the above mentioned solutions.

**Management’s Response (2011):**
An upgrade to the middleware application for IMPACT has allowed us to enforce password length requirements; however, the technology is still unable to address password aging or password history. The additional recommendations to implement password aging and password history features will be implemented as soon as our software platform (Weblogic) allows it or when resources allow for custom changes.

Additionally, note that critical accounts payable functions have migrated from the IMPACT application to PeopleSoft. Early last year, the MTA BSC began to centrally control invoicing and vendor management via PeopleSoft for MTAHQ. In short, PeopleSoft is managing account payable functions, while IMPACT supports budgeting and revenue accounting. The separation of these activities – both functionally and organizationally – has eliminated IMPACT users’ ability to perform operationally sensitive functions.
DEFICIENCIES

We identified, and have included below, deficiencies involving the MTA Business Service Center’s (“MTA BSC” or “BSC”) internal control over financial reporting as of December 31, 2011, that we wish to bring to your attention:

1. Timely Bank Reconciliations

Observation:
Monthly bank reconciliations were not performed on a timely basis. During testing procedures, it was noted that 7 out of 45 monthly reconciliations were completed more than three months after the close of the month (for example a May 2011 reconciliation was not completed until September 2011).

Background:
MTA BSC reconciles bank statements for more than 215 accounts on a monthly basis. The timeliness of these reconciliations is important as the MTA produces interim quarterly financial statements.

It is a goal of the MTA BSC to complete all bank reconciliations on a one month time-lag. At the present time, the average lag is approximately two to three months. However, it was noted that out of the 45 reconciliations selected for testing during the 2011 audit, 7 of these reconciliations were not performed within three months.

Recommendation:
It is recommended that all bank reconciliations be performed within three months.

Management Response:
Management agrees with the recommendations in comments one through three and is proposing a process flow for the BSC and MTA agencies. Adherence to this process this will meet or exceed the recommendations and BSC’s Service Level Agreements (“SLA”). On the next page there is a flow chart detailing the business process.
1. Timely Bank Reconciliations (continued)

Management Response (continued):

- Review GL activity.
- Review Bank Activity.
- Review and prepare list of discrepancies.
- Prepare reconciliation.
- Submit reconciliation for review.
- Supervisor / Senior approves.
- Submit to Agency reconciliation details for their action.
- Agency responds within 10 days.
2. Unreconciled Differences in the Bank Reconciliations

*Observation:*
Monthly bank reconciliations were approved with large unreconciled differences.

During testing procedures, it was noted that 3 out of 45 monthly bank reconciliations were signed off by management as being completed when unreconciled differences had not been resolved.

*Background:*
MTA BSC reconciles bank statements for more than 215 accounts on a monthly basis. The accuracy and completeness of these reconciliations is important as the MTA produces interim quarterly financial statements. Most of the reconciliations are automated. A bank reconciliation is created by running a PeopleSoft query which pulls in the amount shown on the bank statement and then running a second query in PeopleSoft which pulls in the balance shown in general ledger. This information is input into a reconciliation form where the reconciliation is automated and any differences are identified. If no differences exist, the "submit" button is pressed in the bank reconciliation module. If discrepancies exist between the bank and book balances, then the bank reconciliation group must investigate. MTA BSC staff communicates with the appropriate MTA BSC and agency personnel to reconcile the differences.

It was noted that out of the 45 reconciliations selected for testing during the 2011, audit 3 of these reconciliations were approved when unreconciled differences greater than $500,000 existed.

*Recommendation:*
Bank reconciliations should not be approved as completed until all reconciling differences have been resolved and any correctly adjusting journal entries have been posted in the general ledger.

*Management Response:*
BSC approval indicates that the reconciliation is complete, including identification of reconciling items that need Agency research and journal entries. As described in comment one, the proposed business process allows Agencies 10 days to respond to the identified items.
3. Final Bank Reconciliations are not Shared with the Agencies

Observation:
It was noted that final monthly bank reconciliations were not shared with the agencies. This resulted in differences between the ending cash balance per the reconciliation and the amount recorded in the general ledger.

Background:
The MTA agencies depend on the MTA BSC to perform the monthly bank reconciliations for their cash accounts. The MTA BSC uses a bank to book reconciliation approach in which the ending book balance per the reconciliation should agree to the balance recorded in the general ledger.

It was noted on several occasions the ending book balance per the reconciliation did not agree to the amount recorded in the general ledger at December 31, 2011. Per discussion with agency managements, they were never given a copy of the final December 2011 reconciliations to compare them to the amounts recorded in the general ledger.

Recommendation:
All completed reconciliations need be shared with the MTA agencies on a timely basis.

Management Response:
Reconciliations were submitted in 2011 for Agency review. In 2012 the new business process will track the dates of the submissions.
4. Bank Reconciliations Should be Performed at the Agencies

*Observation:*
The bank reconciliation process should no longer be a responsibility of the MTA BSC, but rather a responsibility of the agencies.

*Background:*
Beginning in January 2011, several accounting functions transitioned to the MTA BSC including bank reconciliations. Prior to January 2011, bank reconciliations were performed at the agencies.

Throughout testing during the 2011 audit, there were a number of issues noted including, bank reconciliations not being prepared timely, approval on bank reconciliations with unreconciled differences, and bank reconciliations not being shared with the agencies.

In order to properly reconcile bank accounts, it is imperative that the people performing the reconciliations have knowledge of the daily receipts and payments which allows them to investigate differences timely using the proper resources.

*Recommendation:*
The process of reconciling bank reconciliations should be performed at the agencies and not at the MTA BSC.

*Management Response:*
The Bank Reconciliation process will remain at the BSC. In order to ensure the Bank Reconciliations are done timely without unreconciled differences, a new process is being implemented which was discussed in comment one. Internal Audit will review the process after three months to monitor compliance.
5. Accounts Payable Vendor Master File

Observation:
MTA BSC management does not review the vendor master file periodically for ongoing pertinence and accuracy.

Background:
On January 1, 2011, the MTA BSC took over the accounts payable accounting function for all of the MTA agencies. During the transition of accounts payable to the MTA BSC, the vendor master files maintained at the agencies were transferred to the MTA BSC PeopleSoft system. Prior to this transfer, there was no clean up performed on the files to remove duplicate vendors or vendors that had been inactive for more than one year.

Recommendation:
The accounts payable vendor master list should be reviewed for ongoing pertinence and accuracy. Duplicate vendors should be deleted. Vendors no longer being used or who have gone out business should be deleted from the vendor master list.

Management Response:
The BSC continuously reviews the vendor master file to improve accuracy and pertinence. Since go-live BSC Accounts Payable has been actively identifying and eliminating duplicate vendors. To date the BSC Accounts Payable has made 91,000 vendors inactive. This is an on-going effort and will continue.
6. New Vendor File Setup

Observation:
   a. New vendors were added to the accounts payable vendor master file without a proper Taxpayer Identification Number (“TIN” #).

   b. Information on the Vendor Master Setup- Maintenance Request Form did not agree to what was entered into the PeopleSoft.

   c. New vendors were added to the accounts payable vendor master file when the vendor already existed in the file.

Background:
   a. In order for new vendors to be added to the accounts payable vendor master file, a Vendor Master Setup- Maintenance Request Form must be completed. It was noted that for one vendor a form did not exist. When the Accounts Payable processor was vouching the invoice in the PeopleSoft system, the processor did a search for the vendor in the system and noted no such vendor existed. Then the Accounts Payable processor forwarded the invoice to the Vendor Maintenance team at the MTA BSC to create a vendor in the system. However, an improper TIN # of 9999999999 was entered into the system.

   b. It was noted in two instances where a new vendor was added to the vendor master file and the TIN# per the Vendor Master Setup- Maintenance Request Form did not agree to the TIN # entered into PeopleSoft.

   c. Upon entering a new vendor in the vendor master file, it is MTA BSC policy that a search is conducted in vendor master file to determine if the vendor already exists. Procedures were performed to test the controls around adding new vendors to the master file during 2011. It was noted that out of 45 new vendors tested and subsequently added to the vendor master file, 10 of these vendors already existed in the vendor master file.

Recommendation:
   a. Vendors should not be added to the vendor master file unless a valid TIN #, Social Security # or Employee # has been provided.

   b. A review and approval process needs to be established to ensure that the information on the Vendor Master Setup- Maintenance Request Form is entered accurately in PeopleSoft.

   c. Management needs to enforce the MTA BSC policy of searching the vendor master file before entering a new vendor in order to avoid duplicate vendors.

Management Response:
Management agrees with recommendations.

   a. For ticket refunds and property damage it is not necessary to enter TIN, EIN or Social Security Numbers. For all other transactions, vendors should be added to vendor master file with a TIN, EIN, Social Security Number or Employee ID.
6. New Vendor File Setup (continued)

Management Response (continued):
   b. BSC will create a control report that is reviewed by Quality Control group of all vendor changes on a weekly basis. Target date for implementation is Q3 2012.
   c. BSC AP will ensure the process is strictly enforced.
7. Segregation of Duties

Observation:  
Many employees have access to perform multiple functions within PeopleSoft which creates a segregation of duties issue.

Background:  
a. In the Accounts Payable business area it was noted that there were five employees who were considered a “Superuser” as they had access to (1) add a new vendor, (2) enter a voucher in the system, and (3) initiate a payment request.

b. In the Cash Reconciliation business area two individuals have the ability to enter a voucher in the system or initiate a payment request and also have access to reconcile bank accounts.

c. In addition, certain employees have access to the Cash Reconciliation module (and access to make changes); however, their job responsibilities do not reflect such a need. It was noted that when employees move from one business area to another, user access to particular functions within PeopleSoft is not updated.

Recommendation:  
a. Management should obtain a list from the IT department on a regular basis and review it for pertinence and accuracy. For those employees who no longer require access to a particular function or module in PeopleSoft, management should have such access removed.

b. “Superusers” should be eliminated from all business areas.

Management Response:  
a. Management agrees with recommendation. BSC Accounts Payable management periodically reviews all roles assigned to Accounts Payable roles and staff.

b. All superuser roles have been eliminated.

c. Management agrees and access has been removed.
8. Invoices Not Paid Timely

*Observation:*  
Vendor invoices are not paid timely.

*Background:*  
The MTA BSC policy is to pay vendors within 30 days of receipt of the invoice. The payment date is configured at the vendor level to be net 30 days from the date the invoice is scanned into the Imaging and Process Management ("IPM") scanning system.

It was noted that out of 45 invoices tested during the 2011 audit, 4 invoices were not paid within 30 days of the IPM scan date in accordance with the MTA BSC policy. By not paying invoices timely, the MTA is at risk of incurring interest charges from their vendors.

*Recommendation:*  
All invoices should be paid within 30 days of the IPM scan date.

*Management Response:*  
Management agrees with the recommendations. The four items noted in the Audit were not paid: one was a delay of receipting, one was a funding issue on the purchase order, and two were not paid due to outstanding credits against the Vendor.
9. Vouching Invoices in PeopleSoft

**Observation:**
Invoices received by the MTA BSC were not vouched in PeopleSoft timely.

**Background:**
In accordance with the Service Level Agreement ("SLA") between the MTA BSC and the agencies, the SLA states that all invoices received by the MTA BSC will be vouched in PeopleSoft within 4 business days. If the purchase order information on the invoice is not correct, then the MTA BSC is responsible for contacting the vendor and getting the vendor to correct the information on the invoice and resend to the MTA BSC so it can be vouched in PeopleSoft.

Instances were noted during testing of controls whereby invoices were not vouched within 4 business days from the receipt of the invoice. Invoices need to be vouched timely in order to ensure proper recording of accruals at month, quarter and year-end closes.

**Recommendation:**
All invoices need to be vouched in PeopleSoft within 4 business days in accordance with the SLA.

**Management Response:**
The agreed upon SLA is eight days from receipt of the invoice by Document Management Center ("DMC") to the time it is vouched in PeopleSoft Accounts Payable. BSC internal management reporting indicated that we have been attaining a 97% compliance rate and we will continue to focus on this area.
10. Quality Assurance Review of Vouched Invoices

Observation:
Invoices were not vouched accurately in the PeopleSoft System and the Quality Assurance (“Q&A”) review did not identify such errors.

Background:
On a daily basis a sample of two vouchers are randomly selected from each Accounts Payable processor (about 60 in total per day) and checked for accuracy. The dollar amount, remittance address, invoice number, invoice date, and company name are compared from the invoice to what the processor entered into the PeopleSoft system.

We tested 45 invoices that were selected during the Q&A review and noted 3 instances in which the invoice details did not agree to what was entered into PeopleSoft and no error was noted in the Q&A log book for that day. Discrepancies between the invoice and what was entered into PeopleSoft included (1) different invoice amount, (2) different invoice number, and (3) one voucher that could not be found in PeopleSoft.

Recommendation:
During the daily Q&A review all errors should be noted in the Q&A log. This log should be reviewed by management on a daily basis.

Management Response:
Management agrees with the recommendation and will ensure that the Q&A process of reviewing 7% of all vouchers daily is strictly adhered to. We will re-enforce the training of the Q&A staff.
11. Accounts Receivable Reconciliation and Detail

Observation:
We were unable to obtain detail supporting the year-end accounts receivable general ledger account balances. The only detail that was able to be provided during the audit was the running total of the current year’s activity (all debits and credits made to the account for the year).

Furthermore, there was no evidence of a reconciliation having been performed between the general ledger and the underlying records.

Background:
The accounts receivable balance is a balance sheet account that represents a balance as of a point in time. In order to gain assurance on the balance reported as of December 31, 2011, we must sample on the account balance at that date. Because we were unable to obtain the population comprising the ending balance at December 31, 2011, we had to sample on all account balance activity for the year. This results in a higher sample size and audit inefficiencies.

Furthermore, if management is unable to produce a detail listing of the accounts receivable balance then there is no way to perform a meaningful review of the accounts receivable balance to determine necessary reserves and to follow up on outstanding items.

Recommendation:
Management should create reports that capture the detail comprising the year-end accounts receivable balances.

Management Response:
This comment is specific to the NYCTA’s Work In Progress (WIP, or Unbilled Receivables) account. The transactions on these accounts are recorded both by BSC AR and NYCTA Capital Accounting; BSC AR records the Debits or Unbilled Costs while NYCTA records the credits or Capital Bills issued from this account. Unlike LIRR and MNCR (for which BSC Accounts Receivable Department creates capital bills), NYCTA continues to bill using their Capital Accounting Receivable System (CARS). Since two independent systems are used to generate the entries for the WIP account, neither one of the systems can provide a report of the detail that would support the remaining un billed costs in the Ledger. In the current environment the creation of such a report is not feasible. BSC can work with NYCTA to more fully utilize the BSC’s AR billing system to alleviate this issue.
12. Journal Entries

Observation:
The agencies send journal entries to the MTA BSC to post in the general ledger. There is no confirmation sent back to the agencies notifying them that the MTA BSC has posted the entry in the general ledger.

Background:
All journal entries are posted to the PeopleSoft system by MTA BSC personnel. The agencies have the ability to initiate a journal but cannot post the journal in the system. The agencies inform the MTA BSC when to post the entries in the system.

There is no confirmation sent to the agencies from the MTA BSC notifying them that the entry was posted in the system. This notification is important so that the agencies can review the entry posted to ensure accuracy.

Recommendation:
MTA BSC management needs to notify the agencies when journals are posted in the general ledger.

Management Response:
BSC agrees and this will be implemented in the 3rd quarter of 2012.
13. Database Password Controls

*Observation:*  
It was noted that password configurations at the database level can be strengthened.

*Background:*  
We noted that PeopleSoft is supported by an Oracle database. However, the database parameters for Oracle could be enhanced to provide stronger protection from unauthorized access. Currently, most of the password parameters at the database level are not enabled.

*Recommendation:*  
Management should consider implementing strong password controls at the database level to establish optimal system security. Strong passwords make it difficult for hackers to guess the password and gain unauthorized access to the system and the data within it.

*Management's Response:*  
Management agrees with the recommendation. Although there currently exists a multi-tier approach to security to prevent unauthorized access, which is an industry best practice, database level password control will be implemented by 4th quarter 2012, which will allow us to strengthen the password configuration.

Observation:
It was noted that there are audit logs or procedures in place to capture security events at the PeopleSoft application level. However, there was no evidence for the review of these logs starting November 2011.

Background:
As part of our assessment for the PeopleSoft application, we noted through discussions with management that the monitoring reports are electronically signed by the management. During the November 2011 timeframe, the electronic signature capability used was lost during an upgrade to Windows 7. Therefore, we were unable to obtain evidence of audit log reviews from November 2011 onwards.

Recommendation:
Management should consider documenting and retaining evidence related to their review of the PeopleSoft audit logs. In the absence of electronic signatures, management should develop a manual method to document evidence of their review. The documentation should include details of the review such as date of review, names of personnel whose access is reviewed and sign offs by the manager(s) performing the review.

Management's Response:
This recommendation has been implemented. The electronic signature capability was in place from mid-December 2011.
15. Change Management

Observation:
There is no documentation showing the application changes are tested in a non-production environment prior to migrating them to production. There are no testing plans or results that are maintained.

Background:
As part of our assessment for the PeopleSoft application, we noted through discussions with management, there is currently no documentation being maintained to show the test plans and testing results for the changes to PeopleSoft.

Recommendation:
Management should consider formally documenting testing information for changes occurring at the PeopleSoft application level. The test plans as well as test results should be maintained and stored such that they can be obtained upon request.

Management’s Response:
Management agrees with the recommendation and test plans and results are now required to be documented for all high impact application changes. In addition, the feasibility of procuring an enterprise test tool is currently being researched with the intent to make a decision by the first quarter of 2013.
16. User Access Evidence

**Observation:**
We were unable to get user access request evidence for 1 of the 5 samples selected for testing.

**Background:**
As part of our assessment of the process to gain access to the PeopleSoft application, we obtained a sample of 5 users who were provided access during the year. However, we could not obtain supporting evidence for 1 of the 5 samples. Through further discussions with management, we noted that the access allotted to the individual was appropriate, but the supporting evidence could not be obtained.

**Recommendation:**
Management should store access request related information in a central repository so that information can be retrieved when required. If emails are used as a form of approval for access, then these emails should be archived.

**Management’s Response:**
Management agrees with the recommendation and process has been put in place for storing all access request related information in a central repository.
1. PeopleSoft Training

Observation:
Agency management and staff are not adequately trained to use PeopleSoft.

Background:
Beginning in January 2011, several accounting functions transitioned to the MTA Business Service Center including accounts payable, treasury, fixed assets, general ledger and payroll. Prior to January 2011, these functions were performed by the individual agencies. In conjunction with this transition, the agencies switched their general ledger systems to PeopleSoft. This was required by the agencies in order to view and query information now processed by the MTA Business Service Center.

Numerous PeopleSoft reports were requested during the audits from agency managements. In many cases, agency managements did not know how to run the reports in PeopleSoft or they were uncomfortable running the reports due to lack of training in the new system.

Recommendation:
Agency management and staff requiring PeopleSoft access should be required to attend an additional PeopleSoft training session. The MTA Business Service Center should hold in depth training sessions in live format instructed by well versed PeopleSoft experts.

Management Response (2010):
The MTA Business Service Center provided training via a “train-the trainer” approach to all MTA agencies in late 2010.

To further support the needs of the agencies, additional classes in “Query Manager” were provided to the agencies to ensure that they can write and run reports they require. Each agency has “super users” that can be utilized to run reports or provide on-going training to employees.

Furthermore, on line courses via step-by-step videos were available at startup and continue to be available on the BSC portal as well as on some agency intranet sites. The BSC will provide additional PeopleSoft training as requested by the Agencies.

Status Update (2011):
Throughout the 2011 audit it was still evident that agency managements were not fully trained in using PeopleSoft. Training can be improved in the areas of general ledger account inquiries and report generation.

Management Response (2011):
BSC management agrees and will prepare a quarterly refresher training schedule to be attended by Agency staff.
2. Retrospective Review of Paid and Open Invoices after Year-End

**Observation:**
Agency managements do not perform adequate retrospective reviews of paid and open invoices after year-end to ensure the appropriate accruals were recorded in their year-end financial statements.

**Background:**
Starting in January 2011, all invoices from agency vendors are sent directly to the MTA BSC for processing and payment. The agencies no longer receive copies of the invoices and do not know about the invoices until they have been processed in PeopleSoft by the BSC. After the invoices have been processed in PeopleSoft the agencies then have access in PeopleSoft to retrieve copies of the invoices.

From an accounting perspective, the service period or delivery date drives the accounting treatment. Many instances were noted in which invoices were received by the BSC after December 31, 2010 that had service periods or delivery dates prior to December 31, 2010. These invoices should have been accrued for as a liability by the agencies as of December 31, 2010.

**Recommendation:**
Every agency needs to perform a retrospective review of paid and open invoices after December 31, 2010 to ensure that all invoices have been properly accrued for in the correct accounting period. It is recommended that this review cover at least 60 days after year-end.

To aid the agencies in this process it is also recommended that the accounts payable open invoice report be modified to include delivery date and/or service period in which the invoice relates to. In order to do this BSC staff needs to enter this information into PeopleSoft at the time the invoice is processed in PeopleSoft.

**Management Response (2010):**
The BSC agrees that a retrospective review of paid and open invoices should be performed for the year end accrual process. It is not the BSC’s practice to enter delivery/service dates at the point of voucher creation. The BSC recommends using receipt information to identify the delivery date and/or service period in which the invoice relates to.

When the item is receipted in PeopleSoft the “Goods Receipt Date” must be entered. This is the actual date of delivery or the service period. We will configure the system to make this field required. A query and report will be created that will list paid and open invoices that compares the “goods receipt date” with the invoice date. These reports will enable the Agencies to properly accrue invoices in the correct accounting period. The BSC will update training documents to insure the proper use of this field.

**Status Update (2011):**
The status of this comment remains open. We reiterate our prior recommendation. In order to aid the agencies in this process, it is recommended that the accounts payable open invoice report be modified to include delivery date and/or service period in which the invoice relates to for both operating and capital expenses. In order to address this issue, the BSC staff needs to enter this information into PeopleSoft at the time the invoice is processed in PeopleSoft.
2. Retrospective Review of Paid and Open Invoices after Year-End (continued)

Management Response (2011):
BSC’s 2010 response is still valid. BSC will evaluate the feasibility of complying with this recommendation.
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, 2011, that we wish to bring to your attention:

1. Fixed Asset Capitalizations

Observation:
Beginning in January 2011, parts of fixed assets processes and accounting were transitioned to the MTA BSC. As a result, LIRR reviews and submits to MTA BSC those fixed assets requiring capitalization. Once this information is sent from LIRR to MTA BSC, it is recorded in PeopleSoft transferring construction work-in-progress to a fixed asset category at which time depreciation begins.

Processing of fixed asset information by the MTA BSC began in May 2011. During the months of June thru December 2011 the MTA BSC worked with LIRR to reconcile beginning fixed asset balances and construction work-in-progress schedules. Capitalizations of fixed assets were sent to MTA BSC for processing from LIRR beginning in December 2011. LIRRR continued to send 2011 capitalizations to MTA BSC for processing until February 2012.

Recommendation:
LIRR management should review and submit fixed asset capitalizations timely to the MTA BSC for processing. It is recommended that this information be reviewed by LIRR management and provided to the MTA BSC on a timely basis.

Management’s Response:
Management agrees. LIRR will establish as schedule for capitalizing fixed assets in PeopleSoft with MTA BSC that will transfer construction work-in-progress to a fixed asset category, record depreciation, and provide timely reports. This will be completed in the third quarter of 2012.
2. Information Security- Oracle DB Passwords

Observation:
We noted passwords for user accounts were not set to expiration at Oracle database level (For users in the default profile). Also a lockout after a certain number of unsuccessful attempts was not enforced. No indication to show that password complexity and minimum length settings were in place.

Background:
Password parameters were also not set for the Oracle Database servers supporting Central Support System (“CSS”), Corporate Time and Attendance application (“CTAMS”) and Warehouse Management System (“WMS”) applications (Default profiles).

Recommendation:
Password configurations for the user accounts should be set to complexity, minimum length, history, invalid logon attempts, and expiration so as to make them difficult to guess for hackers. Imposing account lockout after a certain number of invalid login attempts reduces the risk of password hacking via brute force attacks.

Management’s Response:
LIRR Management agrees with this recommendation. The complexity, minimum length, history, invalid logon attempts, and expiration were changed as requested in April 2012 for CSS (TSS), CTAMS and WMS.
3. Information Security- UNIX OS Passwords

**Observation:**
Obtained password settings on in scope database server(s) and noted that only minimum length was imposed on UNIX password levels. Thus the passwords could not be left blank. Other password parameters such as complexity, history, lockouts, expiration are not imposed on in scope UNIX servers.

**Background:**
Password settings on database servers supporting WMS, CTAMS and CSS applications were not set up – except minimum length.

**Recommendation:**
Password configurations for the user accounts should be set to complexity, minimum length, history, invalid login attempts, and expiration. Imposing account lockout after a certain number of invalid login attempts reduces the risk of password hacking via brute force attacks.

**Management’s Response:**
LIRR management agrees with this recommendation. New password configurations that include complexity, minimum length, history, invalid logon attempts, and expiration will be put in place on all the database servers supporting WMS, CTAMS and CSS applications by the 4th quarter of 2012.
4. Privileged Access - Applications

**Observation:**
We noted segregation of duties was not feasible at the CTAMS application domain. Hence the developer also had the responsibility of making changes into production.

**Background:**
Developers have access to implement changes for the CTAMS application. However all developer actions are captured in logs and the logs are available for review.

**Recommendation:**
Developer access to production should be removed if unnecessary.

If the management has a business justification in place to retain developer’s access to production, the management should document the same. A risk acceptance documentation should be in place which accepts the risk of the above observation.

**Management’s Response:**
An analysis for granting the developer’s access to production was performed and a business need has been deemed necessary for CTAMS for system maintenance and support related tasks. A risk acceptance document will be completed and submitted for approval to IT and the CTAMS business owners. This approval process will be performed annually during LIRR’s Annual recertification initiative. Certification for 2012 access was completed in the 2\(^{nd}\) quarter of 2012.
1. Information Security - Oracle Passwords

**Observation:**
We noted the password settings on the Oracle Database level for Kronos did not mandate the following configurations for Database Administrator Accounts ("DBA"):  
1. Minimum Length  
2. Expiration  
3. History  
4. Lockouts  
5. Complexity

**Background:**
Password mandates could not be imposed on application accounts accessing the database due to system limitations. In addition, password parameters for DBA’s were not set for the Oracle Database supporting Kronos application.

**Recommendation:**
Password configurations for the Oracle DBA’s supporting the Kronos application should be set for complexity, minimum length, history, invalid logon attempts, and expiration in order to make them difficult to guess for unauthorized personnel. In addition, imposing account lockout after a certain number of invalid login attempts reduces the risk of password hacking.

**Management’s Response (2010):**
Password settings for expiration and lockouts are configured as recommended. Additional option settings were added in the fourth quarter 2010.

**Status Update (2011):**
This comment has not been corrected and remains open.

**Management’s Response (2011):**
The Kronos application was replaced by the LIRR’s Corporate Time and Attendance application. The CTAMS application leverages improved security credentials. A special DBA PROFILE was created to set the password parameters. This profile has an additional option that will perform a lockout of the DBA user id if it has not been used within 30 days.
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, 2011, that we wish to bring to your attention:

1. Operating and Capital Accruals

Observation:
MNCR management needs to enhance their year-end process for estimating and recording capital and operating accruals.

Background:
MNCR management has a procedure in place to estimate operating and capital accruals as of December 31st for goods and services received, but for which the invoice has not been received. Management obtains input from various departments in developing these estimates. In addition, MNCR management performs a review of open invoices and disbursements paid subsequent to December 31st and determines if additional accruals are necessary for received goods and services for which invoices were received.

However, during the 2011 audit, 3 instances totaling approximately $194 thousand were noted whereby an accrual was not recorded at December 31, 2011 for goods and services received prior to December 31, 2011.

Recommendation:
Management needs to enhance their year-end process for estimating and recording capital and operating accruals to ensure that all amounts are recorded as accruals at December 31st.

Management’s Response:
Management agrees with this recommendation and plans on extending the time period for its procedures in estimating operating and capital accruals.
2. Fixed Asset Capitalizations

*Observation:*
Beginning in January 2011, parts of fixed assets processes and accounting were transitioned to the MTA BSC. As a result, MNCR reviews and submits to MTA BSC those fixed assets requiring capitalization. Once this information is sent from MNCR to MTA BSC, it is recorded in PeopleSoft transferring construction work-in-progress to a fixed asset category at which time depreciation begins.

Processing of fixed asset information by the MTA BSC began in May 2011. During the months of June, July, August and September 2011 the MTA BSC worked with MNCR to reconcile beginning fixed asset balances and construction work-in-progress schedules. Capitalizations of fixed assets were sent to MTA BSC for processing from MNCR beginning in October 2011. MNCR continued to send 2011 capitalizations to MTA BSC for processing until March 2012.

*Recommendation:*
MNCR management should review and submit fixed asset capitalizations timely to the MTA BSC for processing. It is recommended that this information be reviewed by MNCR management and provided to the MTA BSC on a quarterly basis.

*Management's Response:*
Management agrees. Capitalization of fixed assets will be reviewed and submitted more timely. During 2012 capitalizations have already been submitted.
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 (2009):
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.

Status Update (2010):
Maintenance of Way non-stock inventory for the Structures and Communications department located at Harmon is still being tracked on spreadsheets. In addition, there are approximately 8 additional locations in which scrap inventory is being tracked on spreadsheets. All inventory locations should use item number identifiers and track the inventory in the PeopleSoft system.

Management’s Response (2010):
The Structures and Communications non-stock materials at Harmon have been inventoried, but not placed into the PeopleSoft material database as of June 2011 as had been forecast. Initially, plans had been to utilize the existing Maintenance of Way staffing in place at Harmon to gradually implement this process. Unexpectedly, the existing staff has not been available to devote the necessary time to perform this process due to the additional work with the normal processing of material requisitions and the follow up invoice receipting and payment associated with the new MTA Business Service Center. There have also been two key positions vacant.

As a result, the Chief Engineer and the Director – Maintenance of Way Material Management have determined that this task will best be fulfilled by staff of the new Maintenance of Way Materials Management department. Staffing of that department, although underway, is behind schedule due to problems with delayed approvals and salary issues related to the structure within MNR.

At the present time it is expected that sufficient staff will be on board in the new department to complete this task for the Structures and Communications materials by December 31, 2011. The other eight locations will then be addressed.
1. Maintenance Of Way Non-stock Inventory - Structures & Communications at Harmon (continued)

**Status Update (2011):**
Based on discussions with management and our audit procedures performed in 2011, this comment has not been addressed and remains open.

**Management’s Response (2011):**
The Maintenance of Way Materials Management (“MWMM”) Department was not fully staffed until February 2012. They are currently in the processing of obtaining stock numbers for the Structures and Communications material across the operating territory. They have assumed control of warehouses in Mott Haven, Harmon, and Springdale, and will be storing material at these locations. Of the specific material from the audit, which is approximately 1800 items, 45% have been set up in PeopleSoft and inventory adjustments are underway. Of the remaining 55%, roughly half have been processed by MNR and are waiting for the Business Service Center portion to be completed. The other half are being processed by MWMM for entry into the PeopleSoft catalog. Upon completion, inventory adjustments will then be processed for these items as well. This entire process will be completed by December 31st, 2012. At that time, the scrap inventory will then be addressed.
MTA BUS COMPANY
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, 2011, that we wish to bring to your attention:

1. Application User Access Reviews- GEAC

Observation:
No formal documentation relating to the user access reviews for GEAC application was obtained.

Background:
We noted that management has a process in place to review user access rights for the GEAC application. However we could not obtain any documentation relating to the review of the users with access to GEAC in 2011.

Recommendation:
Management should consider formally documenting user access reviews for all applications, and retaining proper sign-offs for these reviews. Any changes in access rights as a result of the review should also be clearly documented. This will help to make sure that user access remains appropriate and as per management’s intentions.

Management’s Response:
The above mentioned documentation does exist, but the need for access to them was miss-communicated between Agency personnel and the external audit staff. All applications security access are reviewed yearly. Documents of the 2011 GEAC MTA Bus review have now been forwarded. GEAC will be decommissioned this year with migration to the Business Service Center PeopleSoft system.
2. Accrued Liabilities

Observation:
The MTA Bus managements do not perform adequate retrospective reviews of paid and open invoices after year-end to ensure the appropriate accruals were recorded in their year-end financial statements. We noted five invoices were not accrued at the year end.

Background:
Starting in January 2011, all invoices from MTA Bus vendors are sent directly to the MTA BSC for processing and payment. MTA Bus no longer receives copies of the invoices and do not know about the invoices until they have been processed in PeopleSoft by the BSC. After the invoices have been processed in PeopleSoft, the MTA Bus then have access in PeopleSoft to retrieve copies of the invoices.

From an accounting perspective, the service period or delivery date drives the accounting treatment. Many instances were noted in which invoices were received by the BSC after December 31, 2010 that had service periods or delivery dates prior to December 31, 2011. These invoices should have been accrued for as a liability by the agencies as of December 31, 2011. We noted that some invoices received had a service or delivery date before the yearend but were not accrued in the related fiscal year.

Recommendation:
MTA Bus needs to perform a retrospective review of paid and open invoices after December 31, 2011 to ensure that all invoices have been properly accrued for in the correct accounting period. It is recommended that this review cover at least 60 days after year-end.

To aid the agencies in this process it is also recommended that the accounts payable open invoice report be modified to include delivery date and/or service period in which the invoice relates to. In order to do this BSC staff needs to enter this information into PeopleSoft at the time the invoice is processed in PeopleSoft.

Management's Response:
MTA Bus Company will request an “open invoice report” (invoices held and not processed into PeopleSoft) from the BSC for a period of at least 60 days after year-end. MTA Bus will review this report and accrue invoices as necessary.
1. 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 (2009):**
Agree. Procedures referenced in ‘Inventory’ recommendation no. 1 will also delineate the documentation required to be provided and retained for interagency transactions.

**Status Update (2010):**
This recommendation is considered partially completed, as MTA Bus is still in process of documenting business process.

**Management Response (2010):**
Inter-agency transactions are currently being reworked by MTA Internal Audit; should have draft business process by end of May 2011 and final approved business process will be completed by third quarter, 2011).

**Status Update (2011):**
This recommendation is considered partially completed, as MTA Bus is still in process of documenting business process.

**Management Response (2011):**
MTA Bus Company along with NYCTA has mutually agreed to a process where each NYCTA invoice would show job order numbers and each job order number would require a sign-off approval. Documentation will include information such as date, depot location; part number, part description, quantity, unit cost and total value are in place.
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, 2011, that we wish to bring to your attention:

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

Kronos/Unified Timekeeping System (“UTS”): Management Concurs. In April 2008, the I-Vault interface with Kronos was implemented. I-Vault updates Kronos with demographic data from the 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 4th 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.

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

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 1st Quarter 2012.

**Target Dates:**
- UTS: 1st quarter 2012.

**Status Update (2010):**
User access provisioning using I-Vault for Unified Timekeeping System (“UTS”) still has not been fully implemented.

**Management Response (2010):**
Implementation was delayed due to staff reassignments to support the BSC. Revised implementation date is 1st Quarter 2012.

**Revised Target Dates:**
1st Quarter 2012

**Status Update (2011):**
User access provisioning using I-Vault for Unified Timekeeping System (UTS) still has not been fully implemented.

**Management Responses (2011):**
Implementation of this phase has been delayed due to the reassignment of TIS resources to support BSC go-live activities, Data Center Consolidation and the relocation of computer operations from the Staten Island Data Center to 2 Broadway and Livingston Plaza Data Centers.

**Target Dates:**
The new target date for this implementation is 2nd Quarter 2013.
2. 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 procedures1 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.
2. 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:
Kronos: Implemented.
UTS: 1st quarter 2012.

Status Update (2010):
No periodic access recertification is currently being performed for the users with access to Unified Timekeeping System (“UTS”) application.

This issue is still open.

Management Response (2010):
Implementation delayed due to staff assignments to support the BSC.

Target Dates:
UTS: 1st quarter 2012.

Status Update (2011):
No periodic access recertification is currently being performed for the users with access to Unified Timekeeping System (UTS) application.

This issue is still open.
2. Expand Periodic Reviews Over Access Controls (continued)

Management’s Response (2011):
Implementation of this finding is dependent on the full connector of UTS to IVault being in place. Once the implementation of that task is complete, user accounts will provision/de-provision automatically.

Target Date:
The revised implementation date is 2nd Quarter 2013.
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, 2011, that we wish to bring to your attention:

1. Amortization of Debt Issuance Costs

Observation:
TBTA is amortizing debt issuance costs over 30 years for Senior and Subordinate debt and 25 years for Certificates of Participation.

Background:
Debt issuance costs are costs associated with issuing debt (loans and bonds), such as various fees and commissions paid to investment banks, law firms, auditors, and regulators. Debt issuance costs incurred in connection with the issuance of long-term debt are capitalized and amortized to interest expense based on the related debt agreements using the straight-line method, which approximates the effective interest method. The unamortized amounts are included in other assets on the balance sheet.

TBTA amortizes all debt issuance costs related to Senior and Subordinate debt over 30 years regardless of the underlying debt agreement.

Recommendation:
Debt issuance costs for each debt issue need to be amortized separately based on the life of that particular bond. For instance if a Senior bond is issued and set to mature in 23 years, then the debt issuance costs should be amortized over 23 years as opposed to 30 years.

Management’s Response:
Staff has been instructed to amortize debt issuance costs over the life of the debt issue and has adjusted the amortization on the bond issue in which this procedure was not followed in 2011, during the first quarter of 2012.
2. Legal Invoices

Observation:
Legal invoices from third party vendors are not sent directly to the MTA BSC for processing and payment. Instead, these invoices are sent to the TBTA where they are reviewed and approved and then forwarded to the MTA BSC for processing and payment.

Background:
Starting in January 2011, all invoices from TBTA vendors are to be sent directly to the MTA BSC for processing and payment. Based on discussions with TBTA management it was discovered that legal invoices did not follow this workflow and instead they are sent directly to the TBTA.

If different processing procedures are followed for different types of invoices, there is a risk that invoices are not being recorded correctly or timely in the general ledger. This is particularly an issue at period closings such as the quarters or year-end.

Recommendation:
In order to ensure consistency in reporting and recording, all invoices should follow the same procedure and be sent directly to the MTA BSC for processing, recording, and payment.

Management Response:
All third party attorneys will be informed to send invoices to the MTA BSC for processing, recording and payment, effective July 2012.
3. Operating and Capital Accruals

Observation:
1. TBTA management needs to enhance their year-end process for estimating capital and operating accruals.

2. Subsequent to December 31, 2011, TBTA management does not perform a retrospective review of accruals by comparing the actual invoice received to the estimate recorded by management.

Background:
1. TBTA management has a procedure in place to estimate operating and capital accruals as of December 31st for goods and services received, but for which the invoice has not been received. Management obtains input from various departments including Engineering and Construction in developing these estimates. However, during the 2011 audit, 8 instances totaling approximately $401 thousand were noted whereby an accrual was not recorded at December 31, 2011, for goods and services received prior to December 31, 2011.

2. Often actual invoices are received after December 31st for which management initially recorded an estimated amount in the general ledger because the actual invoice was not available. While this is appropriate practice, management does not perform a retrospective review or “true up” of the estimated accruals. This is done by comparing actual invoices received to the estimated amounts and making any necessary adjustments in the general ledger.

Recommendation:
1. Management needs to enhance their year-end process for estimating capital and operating accruals to ensure that all amounts are recorded as accruals at December 31st.

2. Management needs to adjust their estimate for operating and capital accruals for known changes such as the receipt of the actual invoice. When an actual invoice is received subsequent to December 31st for which management had recorded an estimate as an accrual, management needs to compare the actual amount of the invoice to the amount of the estimate recorded and make any necessary adjustment.

Management’s Response:
1. The Engineering and Controller’s staffs will jointly strengthen the procedures over the year-end process for estimating capital and operating accruals.

2. The Controller’s Department, as part of the year end accrual process, will adjust accrual estimates to the actual invoice, if received prior to finalization of the Operating Surplus.
4. User Access Reviews (Kronos)

Observation:
User access review documentation for the 2011 audit could not be obtained.

Background:
As part of our assessment for the Kronos application, we noted through discussions with management that user access reviews are conducted for Kronos on an annual basis. However, we were unable to obtain supporting evidence of the review.

Recommendation:
Management should consider performing the user access reviews for Kronos in a timely manner. Documentation relating to the reviews should be retained so that it can be made available when needed. The documentation should include details of the review such as date of review, names of personnel whose access is reviewed and sign offs by the manager(s) performing the review.

Management’s Response:
User access reviews will be performed and documented on a semi-annual basis, commencing with the implementation of the Kronos 6.2 system in August 2012.
5. Database Password Controls (Kronos)

Observation:
It was noted that there are no password parameters enabled at the Kronos database level.

Background:
We noted that the Kronos application is supported by an Oracle database. Currently there are no password parameters enabled at the database level to protect the database from unauthorized access.

Recommendation:
Management should consider implementing strong password controls at the database level to establish optimal system security. Strong passwords make it difficult for hackers to guess the password and gain unauthorized access to the system.

Management’s Response:
The version of Kronos 5.0 that is used currently is limited to Time Keeping Functionality only. In August 2012, Technology staff will upgrade to Kronos 6.2, expanded to include Attendance, Accruals and Leave modules. Following this major upgrade, Technology staff will implement this recommendation under Oracle 11g database and Real Application Clusters (“RAC”) platform. This platform is better suited to implement strong passwords than the present release of Oracle 9i that is in use today.
6. Audit Logs / Security Event Tracking (PeopleSoft –Payroll)

**Observation:**
It was noted that there are no audit logs being generated to capture security events (e.g. security violations, monitoring the use of the system, etc.) at the PeopleSoft application level.

**Background:**
As part of our assessment of the PeopleSoft (Payroll) application, we noted through discussions with management, there is currently no procedure in place to generate and review security logs on a regular basis.

**Recommendation:**
Management should consider generating and reviewing audit logs for critical applications and databases in order to detect certain security events within the system. These audit logs should be generated and reviewed at fixed intervals determined by management. Evidence of such review should be retained so that it can be made available upon request.

**Management’s Response:**
Recommendation was implemented on July 3, 2012
1. Personnel Files related to Claim Liabilities

**Observation:**
It was noted that the underlying claims information provided to the actuary included incident reports that were coded as “open” and should have been coded as “closed.”

**Background:**
When testing the underlying data used by the actuary to calculate the liability related to Loss and Unpaid Loss Reserves, it was noted that the information provided to the actuary by MTA Risk Management, included claims that related to incidents that were recorded in the system as “open” however, such incidents were not in fact “open” and should have been “closed” in the system. In certain cases such incidents dated back more than 10 years.

**Recommendation:**
MTA Risk Management should review all open incidents/claims in the system and for those incidents/claims that are no longer open they should be tagged in the system as “closed.”

**Management’s Response (2010):**
MTA Risk Management is in the process of reviewing all open TBTA incidents/claims in the NYCT WCIS system and applying the appropriate disposition code to reflect that the incident/claim is closed. This change will be reflected in the September 30, 2011, actuarial data.

**Status Update (2011):**
Instances were noted during the 2011 audit where a claim was reported as open when it should have been reported as closed. As such, this comment remains open.

In addition, there is no one at the TBTA who is responsible for open and closed claims handled by third party service providers. Every year we ask the TBTA claims department to produce selected claim files and each year the TBTA claims department is not able to deliver all claims files selected. It is recommended the TBTA claims department name an individual to take responsibility for open and closed TBTA claims files. This person would also work with the MTA Risk Management team on a regular basis.

**Management’s Response (2011):**
MTA Risk Management now reviews the NYCT PLIS System quarterly to insure that all closed claims are so earmarked.

In the mid-nineties, as part of a MTA Headquarters consolidation process, TBTA’s insurance department was eliminated when all TBTA functions relating to worker’s compensation and third party liability claims were transferred to MTA Risk Management and NYCT Legal. TBTA has since regained responsibility for managing workforce availability and has added one staff member to schedule medical exams and appropriate follow-up; all other workers’ compensation functions, such as management of the PLIS System, are performed by MTA Risk Management and NYCT Legal. Thus, there is no staff at TBTA available to perform the above mentioned recommended procedure.
PRIOR YEAR COMMENTS ADDRESSED
PRIOR YEAR COMMENTS ADDRESSED

Metropolitan Transportation Authority- Headquarters

1. Arbitrage Rebate Calculation- 2010
2. Classification of Unamortized Bond Discount and Premium- 2010
3. PeopleSoft New User Authorization- 2010
4. PeopleSoft Application & Database Password Configuration- 2010
5. PeopleSoft Application Change Management- 2010
6. Opening Bank Accounts- 2010

MTA Business Service Center

1. Imaging and Process Management (“IPM”) System- 2010

First Mutual Transportation Assurance Company

1. Loss Escrow Accounts- 2010

Long Island Rail Road Company

1. Information Security – Privileged Access - 2010
2. Information Security – Security Monitoring - 2010

Metro-North Commuter Railroad Company

1. PeopleSoft New User Access - 2010
2. Crew Management System (“CMS”) User Access Reviews - 2010
3. CMS Database Audit Reports - 2010
4. PeopleSoft Database (Oracle) - 2009
PRIOR YEAR COMMENTS ADDRESSED

Metropolitan Suburban Bus Authority

1. Structured Query Language (“SQL”) Password Controls- 2010
2. Audit Logs / Security Event Tracking- 2010
3. Change Management- 2010
5. Information Security- Password Controls- 2009

MTA Bus Company

1. Application User Access Reviews- 2010
2. Password Controls- 2010
3. Change Management- 2010

New York City Transit Authority


Staten Island Rapid Transit Operating Authority

None

Triborough Bridge and Tunnel Authority

1. Capitalized Payroll - 2010
2. Information Security- User Access Reviews- 2010
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.

* * * *