The Metropolitan Transportation Authority
Report to Management
Year Ended December 31, 2014
April 29, 2015

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, 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, 2014 (on which we have issued our reports dated April 29, 2015, which contain an explanatory paragraph that the MTA requires significant subsidies from other governmental entities), 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 and other matters as of December 31, 2014, that we wish to bring to your attention.

We also plan to issue our reports dated April 29, 2015, in accordance with Government Auditing Standards and OMB Circular A-133 which will include (1) Independent Auditors’ Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with Government Auditing Standards and (2) Independent Auditors’ Report on Compliance for Each Major Federal Program; and Report on Internal Control Over Compliance Required by OMB Circular A-133, that will include a certain matters involving the MTA’s internal control over financial reporting that we considered to be significant deficiencies under standards established by the AICPA.

The definition of a deficiency, a material weakness, and a significant deficiency are 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 of the financial statements 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, Federal
awarding agencies or pass-through entities, 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]

[Debit : Touche LLP]
# Table of Contents

## APPENDIX A

<table>
<thead>
<tr>
<th>Organization</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metropolitan Transportation Authority- Headquarters</td>
<td>6</td>
</tr>
<tr>
<td>MTA Business Service Center</td>
<td>19</td>
</tr>
<tr>
<td>First Mutual Transportation Assurance Company</td>
<td>28</td>
</tr>
<tr>
<td>Long Island Rail Road Company</td>
<td>31</td>
</tr>
<tr>
<td>Metro-North Commuter Railroad Company</td>
<td>34</td>
</tr>
<tr>
<td>MTA Bus Company</td>
<td>38</td>
</tr>
<tr>
<td>New York City Transit Authority</td>
<td>41</td>
</tr>
<tr>
<td>Staten Island Rapid Transit Operating Authority</td>
<td>49</td>
</tr>
<tr>
<td>Triborough Bridge and Tunnel Authority</td>
<td>51</td>
</tr>
<tr>
<td>Prior Year Comments Addressed</td>
<td>70</td>
</tr>
</tbody>
</table>

## APPENDIX B

<table>
<thead>
<tr>
<th>Definition</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definitions: deficiency, material weakness, and significant deficiency</td>
<td>72</td>
</tr>
</tbody>
</table>
APPENDIX A
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, 2014, that we wish to bring to your attention:

1. Backup Monitoring

   **Criteria:**
   Backup processes are monitored for successful execution. Failures are escalated in order to be corrected to ensure data is usable, available for retrieval, and restored if needed.

   **Condition:**
   Documentation for 2 of 15 failed backups was not available.

   **Effect:**
   Financial data cannot be recovered or accessed in a timely manner when data is lost.

   **Recommendation:**
   We recommend the MTAHQ reinforce data center procedures to ensure documentation is retained for all failed backups.

   **Financial Statement Impact:**
   No Impact

   **Management Response:**
   MTA has recently re-organized and consolidated all IT functions including data backup and recovery within the MTA IT Data Center Operations division. This division will be implementing automated processes to monitor data backups. The division will also institute processes to restart failed backups when possible. Root cause analysis will be performed for all failed backups in order to develop corrective actions.
2. User Access Revocation

Criteria:  
User access to the systems is removed upon employee termination.

Condition:  
9 terminated users retained access to the Impact System after their termination.

Effect:  
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access impacting data and the computer-generated information and/or automated controls.

Recommendation:  
We recommend that the MTAHQ improve/revise the user access de-provisioning process and control over timely removal of access in information systems.

Financial Statement Impact:  
No Impact

Management Response:  
MTA will develop scripts to compare active employees from the MTA’s Human Resources systems with registered users in the Impact system, if the HR system indicates that an employee is in a terminated status the user will be automatically inactivated in the Impact System.
3. Change Management- Impact Application

Observation:
D&T noted that two of the developers had access to the source code and the production environment.

Background:
Three developers (programmers) had access to the Impact Source code, two of the developers had access to the source code and to the production environment.

Recommendation:
Management should restrict programmer access to the production environment. Programmers should not be allowed to make direct changes in the production environment.

Management’s Response (2012):
Access to production will be revoked from the Development staff. Access will now be given to the Quality Assurance and Database groups for moving of code into production. A document will be produced with a clear delineation of roles.

Status Update (2013):
The identified observation still remains open.

Two individuals have development and administrative access in production Impact environment giving them ability to develop and implement their own changes in to production without due approval.

We reiterate our prior recommendation.

Management’s Response (2013):
An individual from Quality Assurance (QA) will be trained in the process of deploying new versions of the Impact application and will become the primary and normal means of deploying changes to production. Access will be revoked from these developers once QA can assume full responsibility for WebLogic administration.

Status Update (2014):
The identified observation still remains open.

The developers continue to possess administrative access within the production environment giving them ability to develop and implement their own changes.

We reiterate our prior recommendations.

Management’s Response (2014):
As part of the MTA’s consolidation of all IT functions, administrative access granted to developers in the Impact production environment will be revoked. The Impact production migration function will now be performed by the MTA IT Data Center Operations division beginning in the 3rd quarter of 2015 as part of an ITIL based change management process.
4. 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. In addition, many governments face the challenge of offering competitive compensation packages to entice strong candidates to come work for 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.

- 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 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.
4. Succession Planning (continued)

- 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 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.
4. Succession Planning (continued)

Management Response (2011):
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.

Status Update (2012):
While some progress has been made during 2012, this comment remains open.

It is recommended that the MTAHQ implement a strategic approach to succession planning in all departments and at all levels. In addition, MTAHQ should ensure that competitive compensation packages are in place in order to entice strong, competent, and talented candidates to come work MTAHQ.

Management’s Response (2012):
MTAHQ is in the process of hiring a Director of Organization Development who will, among other initiatives, spearhead a succession planning program that will address the issues highlighted in Deloitte’s report. In addition, the following additional steps are being conducted to address this matter:

1) MTAHQ is identifying mission critical positions that are hard to fill because of the requirements of job or may become vacant due to retirements.
2) MTAHQ is conducting an age/years-of-service analysis by Department and by individual to project upcoming attritions due to retirements.
3) MTAHQ continues to work with the Business Service Center on the development of a Talent Management System that identifies high potential employees not only within the MTAHQ but within other MTA entities to fill positions as they are identified. This system will leverage existing PeopleSoft modules.

Status Update (2013):
While some progress has been made to ensure that the proper strategic approach to succession planning at all levels, including the identification of mission critical positions, focus should continue in this area. Therefore, we reiterate our 2012 recommendation.

Management Response (2013):
MTAHQ has hired a talent management leader to lead HQ talent management and related programs such as succession planning and talent development.

The effort to deploy succession planning is now part of a broader talent management strategy encompassing talent assessment, talent development, and succession management (which includes key position identification, succession planning, and talent review). Key components of this effort are now being put into place. Key talent management leaders in each agency have been identified and are now involved with streamlining the PeopleSoft system to create a centralized repository for employee information used for talent management purposes.
4. Succession Planning (continued)

Management Response (2013):
In the talent assessment component, we’ve purchased licenses for use of a proprietary competency model and trained Agency talent management leaders in its use. This model will be used to assess key employee capability in core MTA competencies. These key employees will become part of an MTA talent pool used to fill key positions. After assessing key employees in the talent pool, we’ll be in position to identify common development needs of these employees and execute a strategy to shore up the identified needs via training or experiential activities (talent development component). Critical individual development needs will also be addressed within this component.

In the succession management component, we’ve now completed the identification of key positions. Next steps will be to conduct formal talent reviews in each of the organizations. During the talent review process, we’ll have discussions with each of the management teams on the capability and availability of talent for each of the key positions. In areas where capability gaps exist, the managers will implement a strategy to shore up these gaps through planned development activities. During talent review, managers will also assess availability of talent for particular roles. Where feasible, they will decide to build capability by rotating talent to new roles to facilitate acquisition of key skillsets via experience. In some cases, the managers will determine that the most effective way to address a particular talent shortage will be via external hire. Execution of internal development strategies coupled with external hires will assure availability of successors for key positions.

Status Update (2014):
While progress has been made over the past several years, this comment remains open.

Management Response (2014):
We agree with this recommendation. As noted in the prior year’s management’s response we are in the process of developing the key components for succession management and will continue to make this a high priority for the MTA.
5. Audit Logs / Security Event Tracking- Impact Application

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 (2011):
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.

Status Update (2012):
This comment has not been corrected and remains open.

Management’s Response (2012):
Starting in June 2013, QA will be provided with WebLogic log information that will produce relevant information about failed logon attempts. QA will then alert EITG and customer management of the aforementioned violations.

Status Update (2013):
This comment has not been corrected and remains open.

MTAHQ did not log and track security events that occur within the application during 2013. Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases risk of unauthorized access affecting data that underlie computer-generated information and/or automated controls.

We reiterate our prior recommendation that MTAHQ enable the Impact System to track security events. In addition, management should also establish procedures to review event logs to ensure unauthorized events are captures and resolved in timely fashion.
5. Audit Logs / Security Event Tracking- Impact Application (continued)

Management’s Response (2013):
It is not clear what type of “unauthorized events” are expected to be captured via Impact’s WebLogic (WL) logs. Impact is an intranet application and can therefore only be accessed via authorized network users. Unauthorized network users can’t get to the network and therefore will never reach the WL logs. The only failed login attempts that make it to logs are authorized network users who don’t have access to Impact. In this case, after 5 failed login attempts, WL locks the user id (assuming it’s a valid user id) which prevents unauthorized access.

In order to address this concern, a report has been created that will be run periodically and will notify QA of all failed login messages in the logs.

Status Update (2014):
This comment has not been corrected and remains open.

MTAHQ did not log and track security events that occur within the application during 2014. This increases the risk of unauthorized access impacting data and the computer-generated information and/or automated controls.

We reiterate our prior recommendation that MTAHQ enable the Impact System to track security events. In addition, management should also establish procedures to review event logs to ensure unauthorized events are captured and resolved in timely fashion.

Management’s Response (2014):
After clarification, MTA IT is defining “security events” as the change to a user’s authorization level within the IMPACT Application. IMPACT uses roles to authorize a particular user to be able to perform a specific function. For example a role may allow “read only” access which would allow a user to only view data while logged on to the systems. Other roles may grant the authority to submit data while others may allow for approvals within a specific workflow. System owners have the primary responsibility of assuring that only appropriate roles are granted to staff for the performance of their job functions.

In order to assist system owners with this responsibility audit information for all changes to role assignments in the IMPACT Application will be recorded in audit tables. Reports will be developed and issued monthly to user management detailing all changes to role assignments which have been made in the past month. This functionality will be included in the IMPACT by the end of the 3rd quarter of 2015.
6. 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 signoffs by the manager(s) performing the review.

**Management’s Response (2011):**
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.

**Status Update (2012):**
This comment has not been corrected and remains open.

**Management’s Response (2012):**
QA will now be responsible for adding, modifying and deleting WebLogic access for users of the Impact application. A recertification process will be done each January to confirm validity of User access. All Agency Help Desks will be informed at that time that all users that have not accessed Impact for one year will be deleted.

**Status Update (2013):**
This comment has not been corrected and remains open.

MTAHQ did not perform a review of users with access to the Impact application in 2013. Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases risk of unauthorized access affecting data that underlie computer-generated information and/or automated controls.

We reiterate our recommendation that MTAHQ establish procedures to perform periodic user access reviews to ensure users have appropriate access within the application to perform their day-to-day job responsibilities and to also ensure user access remains appropriate.
6. User Access Reviews- IMPACT Application (continued)

Management’s Response (2013):
The determination of which users have which authorities does not belong to the IT group, but to the business user departments. They currently have forms and approval processes in place that are required in order to grant user access and authorities.

That being said, the following changes are being made to address this concern. The QA department will be responsible for the addition and deletion of Impact users from WebLogic. In addition, a report will be sent once a year to the business user departments identifying all user ids that have not accessed the Impact application within the last year. After sufficient time for review, these user ids will be inactivated.

Status Update (2014):
This comment has not been corrected and remains open.

MTAHQ did not perform a review of users with access to the Impact application in 2014. Due to the increased risk of unauthorized access impacting data and the computer-generated information and/or automated controls, we reiterate our recommendation to establish procedures to perform periodic user access reviews.

Management’s Response (2014):
Currently the responsibility of reviewing and validating user authorization has been delegated to system owners not the IT department. The creation of an annual report to identify any user who has not accessed the Impact application within the last year has been completed.

In order to seek to be proactive and assist system owners in validating authorization, IT will investigate the possibility of accessing the MTA’s HR system to try to determine when a user’s position has changed and therefore alerting system owners when a review of authorizations is warranted.
OTHER MATTERS

Other matters related to our observations concerning operations, compliance with laws and regulations, and best practices involving internal control over financial reporting that we wish to bring to your attention are as follows:

7. Financial Statement Drafting

Criteria: 
n/a

Condition:
The management’s discussion and analysis (MD&A) and footnotes to the financial statements vary from entity to entity within the MTA organization.

Cause:
Each entity within the MTA has a separate and distinct financial reporting process.

Effect:
The MD&A and footnotes to the financial statements are not consistent between MTA entities.

Recommendation:
1. The MTA should hold a financial statement drafting session that focuses on the MD&A and the footnotes.
2. Related to the MD&A, management should strive to communicate what is important to those who want to understand the various operations of the organization like fare box recovery and how it compares to other transportation systems in the country. Management should also draw attention to “big ticket” items that drive cost like pensions, OPEB and salary increases. Management should then focus on the transparency of the related party transactions and the financial transactions between entities. While each report should be similar and discuss topics in the same order across all of the entities, each report also needs to cover what is unique or important to each entity.
3. The footnotes should be in a common order and standardized wherever possible. The goal is to reduce the time needed for each entity to complete their financial statements. If there are changes during the financial reporting process, they can be quickly incorporated into all the entity reports. This process will involve input from every agency.
4. Enhance the related party disclosures to ensure maximum transparency and consolidate the disclosures into one footnote.

Financial Statement Impact:
No Impact

Management Response:
We agree with this recommendation. In July a project committee of Agency Controllers led by Internal Audit will be reviewing all of the Agency and Consolidated financial statements for consistency and comparability in the disclosure in the MD&A and, footnotes as well as standardization in the basic financial statements.
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, 2014, that we wish to bring to your attention:

1. Vendor Master File

Criteria:
Changes to the vendor master file are processed timely.

Condition:
When a new vendor is added to the vendor master file or if changes are requested to an existing vendor, the requesting Agency completes form “FIN-AP-023 Vendor System Master Maintenance Request Form.” The approved form is submitted via fax/email to the Document Management Center (“DMC”), who scans and transmits the form to an Accounts Payable processor for input into the vendor master file. There is a standard letter of agreement between the MTA BSC and the MTA Agencies that vendor master set-up should be processed within 4 business days upon receipt of the scanned form.

Cause:
During 2014, PRGX was contracted by the MTA BSC to perform a vendor master file clean up. As part of the service provided by PRGX, the FIN-AP-023 forms were sent to a separate and distinct PRGX web portal which interfaced with the PeopleSoft system. However, during 2014, FIN-AP-023 forms were sent directly to MTA BSC portal.

Effect:
As a result of the FIN-AP-023 forms being sent to the incorrect web portal, a large backup of unprocessed vendor changes was created.

Recommendation:
Management should review the existing process for submitting vendor changes. Management should ensure that all changes to the vendor master file are processed within 4 business days of receipt of the FIN-AP-023 form.

Financial Statement Impact:
No Impact

Management Response:
The engagement of PRGX was in part an effort to clean up the Vendor Master files which at the BSC’s go live was a compilation of several large and incongruent Vendor Master Files from the Agencies. PRGX’s initial contact with vendors was to update the information that was in the BSC’s Vendor Master File. Vendors were directed to return FIN-AP-023 forms to a different portal when updating just information; this was intentional so as not to impede the normal processing of payments. The overwhelming response did create a temporary backlog but at no time did this prevent the processing and payments to be made timely or accurately.
2. Backup Monitoring

*Criteria:*  
Backup processes are monitored for successful execution. Failures are escalated in order to be corrected to ensure data is usable, available for retrieval, and restoration if needed.

*Condition:*  
Documentation for of 2 of 15 failed backups was not available.

*Effect:*  
Financial data cannot be recovered or accessed in a timely manner when data is lost.

*Recommendation:*  
We recommend the MTA BSC re-inforce data center procedures to ensure documentation is retained for all failed backups.

*Financial Statement Impact:*  
No Impact

*Management Response:*  
For two of the days (5/16 and 12/3) there was an issue with the tape library and the IBM consulting engineer had the library take the backup offline to perform the repairs. This caused the backups to run past the windows for pickup for each day. The standard operating procedure in this situation is that the tapes are ejected from the library stored in locked cabinets in the data center and then sent offsite the next day. This is what occurred in the situation.
3. PeopleSoft Access to Modules

**Criteria:**
Access to the following PeopleSoft modules is restricted based on job function:

a) Bank Reconciliations  
b) Accounts Payable  
c) Payroll  
d) Human Resources  
e) Fixed Assets  
f) General Ledger

Individuals do not have access to the aforementioned modules if not required to perform their daily job functions.

**Condition:**
Users who do not require access to a particular module in PeopleSoft had access to make changes. We obtained reports from the Information Technology department to determine the last time the users accessed these particular modules in PeopleSoft. We viewed change reports to ensure these users had not made unauthorized changes in the modules. While we noted no changes were made to these particular modules by these users, it is a risk to the MTA and the Business Service Center when individuals have access to modules in PeopleSoft and such access is not a requirement for the users to perform their daily job functions.

**Cause:**
User access review for all modules contained within PeopleSoft are not periodically reviewed to determine if user access is still required.

**Effect:**

a) Bank Reconciliations- It was noted that 8 individuals had access to the bank reconciliation module when access was not required to perform their daily job functions.

b) General Ledger- It was noted that 9 individuals had access to initiate a journal entry in the general ledger module when access was not required to perform their daily job functions.

c) General Ledger- It was noted that 8 individuals had access to post a journal entry in the general ledger module when access was not required to perform their daily job functions.

**Recommendation:**
Management should review user access privileges for all modules in PeopleSoft on an annual basis (or more frequently if deemed necessary). This review should ensure that users who do not require access to a module to perform their daily job functions are not making unauthorized changes.
3. PeopleSoft Access to Modules (continued)

Financial Statement Impact:
No Impact

Management Response (2013):
Management agrees and will review user access privileges annually. It also should be noted that some individuals will retain certain access that may be required due to processing requirements. The dynamics of the work environment user access is granted when needed and subsequently revoked when no longer necessary.

Status Update (2014):
While progress was made during 2014 to eliminate user access in PeopleSoft for users who do not require access to perform their daily job functions, the following was noted during 2014:

   a) Cash module- 2 individuals had access to the cash module when access was not required to perform their daily job functions.

   b) Accounts Payable module- 1 individual had access to add a vendor to the master vendor file and also had access to input a voucher in the accounts payable module when access was not required to perform his daily job function.

Management Response (2014):
Access for these three individual has been corrected. Management agrees with the recommendation and does review access annually. It should be noted that access is granted when needed and revoked subsequently.
4. User Access Reviews- PeopleSoft Application

**Observation:**
User access reviews for the PeopleSoft application was not performed during the period. No documentation evidencing the user access review could be obtained.

**Background:**
It was noted that formal documentation relating to user access review for the PeopleSoft application was not available during the period.

**Recommendation:**
Management should consider documenting evidence for the user access reviews for PeopleSoft. 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 (2012):**
This information was not requested from BSC Information Technology as part of the audit. User activity reviews for the BSC PeopleSoft system are performed on a weekly basis. User recertification is performed annually.

**Status Update (2013):**
The identified observation still remains open as of December 31, 2013.

The MTA BSC management team initiated their annual user access review however their reviews were not completed by December 31, 2013. This could result in users having access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.

We reiterate our prior recommendation above. In addition we recommend that MTA BSC establish procedures to monitor the progress and completion of the PeopleSoft user access reviews to ensure all reviews are completed within the required timeframe.

**Management Response (2013):**
Recertification for 2013 was started early this year using recommended audit suggestions from a recent MTA HQ audit. These include finalizing the role descriptions for the PeopleSoft modules, finalizing the risk classification for these roles and implementing the use of queries to automatically recertify users for low risk privileges in PeopleSoft. Furthermore data owners will perform the recertification, advise the department head of the results and resolve any differences before sending it to MTA BSC IT Security. The revised process is documented in the form of a comprehensive detailed procedure specifying naming conventions for files and directories and detailed actions to be taken.

**Status Update (2014):**
The identified observation still remains open as of December 31, 2014.

We reiterate our prior recommendation above. In addition we recommend that MTA BSC establish procedures to monitor the progress and completion of such reviews to ensure all reviews.
4. User Access Reviews- PeopleSoft Application (continued)

*Management Response (2014):*
Management is in agreement with the comment and will establish procedures to comply with the Audit recommendation.
5. 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 (2011):
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.

Status Update (2012):
There are still instances in which vendor invoices are not paid timely. As such, this comment remains open.

Management Response (2012):
The timely payment of invoices is contingent upon Agency receipt of the goods or services being in the system, processing of the invoices by BSC and having the funding available in Procurement. The BSC provides to the Agency on a weekly basis a summary of all vouchers in the system that have not been paid yet and the reason for that non-payment. BSC will continue to work with the Agencies to improve the timeliness of invoice payments.

Status Update (2013):
There are still instances in which vendor invoices are not paid timely. As such, this comment remains open.

Management Response (2013):
All invoices should be paid the later of 30 days after invoice date or receipt of goods or services. In 2012 and 2013 Prompt Payment was $208,805 and $53,068 respectively. The BSC continues to work with the agencies to expedite the payment process. In 2013, our monthly analysis indicated that approximately 70% of the delayed payments are due to missing receipts. This data is provided to the MTA agencies accounting department weekly in order for the agencies to take action.

The BSC also provides to Procurement and expedites a detail analysis of all vouchers that have not been paid and a reason code that identifies the issue.
5. Invoices Not Paid Timely (continued)

**Status Update (2014):**
There are still instances in which vendor invoices are not paid timely. It is suggested that MTA BSC work with the MTA agencies to ensure that receipts are entered into PeopleSoft timely to ensure timely payments to the vendors.

**Management Response (2014):**
The timely and accurate payment of invoices is the goal of the BSC Accounts Payable department. As stated in previous responses that goal is only accomplished when all relevant parties are participating in achieving that goal. To assist in the timely processing of payments the BSC provides reports to Agency Procurement Departments and user departments, a detailed analysis of all vouchers that have not been paid and a reason code that identifies the issue. These reports contain the items that if no action is taken will not be paid timely. We will continue to review our procedures and refine our internal reporting toward achieving the goal.
FIRST MUTUAL TRANSPORTATION ASSURANCE COMPANY
DEFICIENCIES

We identified, and have included below, deficiencies involving the First Mutual Transportation Assurance Company’s (“FMTAC”) internal control over financial reporting as of December 31, 2014, that we wish to bring to your attention:

1. Writing Insurance Premium Policies

Criteria:
Governmental Accounting Standards Board (“GASB”) Codification of Governmental Accounting and Financial Reporting Standards (“GASB Codification”), Section Po20.116, Premium Revenue Recognition, states the following:

Premiums or required contributions ordinarily should be recognized as revenue over the contract period in proportion to the amount of risk protection provided. For those few types of contracts for which the period of risk differs significantly from the contract period, premiums should be recognized as revenue over the period of risk in proportion to the amount of risk protection provided. That generally results in premiums being recognized as revenue evenly over the contract period (or the period of risk, if different), except for those few cases in which the amount of risk protection changes according to a predetermined schedule.

Condition:
During testing of insurance premium revenue, all of the insurance premium policies (contracts) written in 2013 were requested to be provided by management. Upon receipt of the policies, it was noted that four had not been officially written, approved, or signed by FMTAC management in a timely basis. This approval process was initiated in March 2014 and finalized in April 2014, at which time they were provided to Deloitte. Therefore, at the time of the revenue recognition (2013), there was no formal documentation supporting the recording of such revenue.

Cause:
FMTAC did not effectively plan and execute the signing of the new insurance policies prior to the expiration of the old insurance policies.

Effect:
Insurance policies were not written, approved, and signed by FMTAC in a timely manner.

Recommendation:
All of FMTAC’s insurance policies need to be written, approved, and signed by management in a timely manner.

Financial Statement Impact:
No Impact

Management Response (2013):
Management agrees with recommendation. The delayed issuance of the four policies was due to a one-time restructuring of the policy form. Management’s priority will be timely issuance of all FMTAC policies.
1. Writing Insurance Premium Policies (continued)

Status Update (2014):
A final signed MetroCat policy including the additional flood surge protection was not available as of April 2015. We noted, however, that it is included in the reinsurance agreement, and we further noted that informal documentation exists with respect to the agreement between FMTAC and MTA. However, as it does not cover the final year of the three-year policy ending June 2016, this comment remains open.

Management Response (2014):
Management agrees with recommendation. Management’s priority will be to clearly document the final year of the additional flood surge protection between FMTAC and the MTA.
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, 2014, that we wish to bring to your attention:

1. **Assets Not Capitalized Timely**

   **Criteria:**
   Generally accepted accounting principles require the proper and consistent capitalization of expenditures to comply with periodicity and the matching principle.

   **Condition:**
   It was noted that Project Managers did not communicate timely the capitalization status of certain projects to the Controller’s office.

   **Cause:**
   Due to a breakdown in communication between the Project Managers and the Controller’s office, capital projects were not transferred timely from the “work-in-progress” category into capitalized fixed assets when the projects reached beneficial use.

   **Effect:**
   “Capital assets not being depreciated” were overstated in the financial statements, while “Capital Assets being depreciated” and “Depreciation Expense” were understated.

   **Recommendation:**
   It is recommended that the Controller’s office and Project Managers communicate timely and periodically on projects’ status and date beneficial use is reached, to ensure capitalization of fixed assets in the correct period.

   **Financial Statement Impact:**
   There was no material impact to the LIRR’s financial statements as of December 31, 2014.

   **Management Response:**
   A quarterly review of all projects in PIP will commence starting after Q1 2015. Review will identify the scope of the project (i.e. study, design construction, etc.,) with the expected beneficial use dates. If construction phase has been completed Project Managers to confirm completion by completing beneficial use form.
2. Annual User Recertification Review

Criteria:
User access privileges are periodically reviewed by application owners to make sure access privileges remain appropriate.

Condition:
An annual recertification process is implemented and takes place during the first quarter of the following year; however, we noted that the annual user access recertification process was initiated but was not completed as of March 26, 2014.

Cause:
LIRR did not complete annual recertification in timely fashion.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases risk of unauthorized access affecting data that underlie computer-generated information and/or automated controls.

Recommendation:
Management should establish procedures to ensure that user access reviews are initiated and completed within a timely manner.

Financial Statement Impact:
No Impact

Management Response (2013):
Recertification occurs annually and is conducted by the security group within the LIRR Information Technology Department. The 2013 recertification was initiated in January 2014 for the year ended December 31, 2013, and has been completed as of May 29, 2014.

Status Update (2014):
The identified observation still remains open as of December 31, 2014.

We reiterate our prior recommendation above. In addition, we recommend that MTA LIRR establish procedures to monitor the progress and completion of such reviews to ensure all reviews.

Management Response (2014):
The recertification process was delayed due to personnel transfers and is now in progress. We expect to have the entire process completed by the end of the 3rd QTR 2015.
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, 2014, that we wish to bring to your attention:

1. Assets Not Capitalized Timely

Criteria:
Generally accepted accounting principles require the proper and consistent capitalization of expenditures to comply with periodicity and the matching principle.

Condition:
It was noted that Metro-North Commuter Railroad Company (the “Company”) Management delayed capitalization of fixed assets for the third quarter of 2014 until the fourth quarter of 2014.

Cause:
Due to a temporary vacancy in the accounting department, coupled with preparation for the Company’s office relocation, Management decided to delay recording of capitalization of fixed assets in the third quarter of 2014. The Company did not submit to the MTA Business Service Center (“BSC”) the report of the “work-in-progress” assets that had fulfilled the appropriate requirements to be capitalized and “placed-in-service” for the purpose of calculating depreciation as of September 30, 2014.

Effect:
As of September 30, 2014, “Capital assets not being depreciated” were overstated on the financial statements, while “Capital Assets being depreciated” and “Depreciation Expense” were understated. During the fourth quarter of 2014, capitalization for all assets was recorded, including for the third quarter items. Depreciation expense was properly recorded for all fixed asset items based on their actual “in-service” date.

Recommendation:
It is recommended that Management review and record all transactions related to capitalization and depreciation accurately and timely. This will ensure that accounting records are accurate, and items are appropriately classified and depreciation calculated in the correct period. It is further recommended that the required information be reviewed by Company Management and provided to the BSC on a quarterly basis.

Financial Statement Impact:
There was no material impact to the MTA’s quarterly consolidated financial statements as of September 30, 2014. As assets were properly classified, and depreciation expense properly recognized during the fourth quarter of 2014, there was no impact to the Metro North Commuter Railroad Company’s or to the MTA’s consolidated financial statements as of December 31, 2014.

Management's Response:
Management agrees. Capitalization of fixed assets will be submitted to the BSC each quarter. All information is reviewed by management prior to submission to the BSC.
2. User Access Revocation – CSS application

Criteria:
Access for terminated and/or transferred users is removed or modified in a timely manner in accordance with the documented company policy.

Condition:
Three (3) terminated users retained access to the CSS application. The access was terminated per notification to the IT department.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access impacting data and the computer-generated information and/or automated controls.

Recommendation:
We recommend the MNCR improve/revise the user access de-provisioning process and control over timely removal of access in the information systems.

Financial Statement Impact:
No Impact

Management Response:
We agree with the recommendation. Metro-North currently has a process in place to address account management changes. When an employee separates from the company the account is immediately disabled upon notification. A weekly report is generated to monitor employment status changes and action is executed upon the findings in the report. This report will be generated on a daily basis and action executed daily for a more frequent review of employment status changes.
3. Privileged-level access

Criteria:
Privileged-level access (e.g., security administrators) is authorized and appropriately restricted.

Condition:
Four (4) accounts listed as "Enterprise Administrators" and six (6) accounts listed as "Domain Administrators" were deemed inappropriate. The Enterprise and Domain accounts are system accounts that were created/enabled to be utilized during the ongoing merger of the IT departments across the agencies.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to the lack of established security policies and standards. This increases risk of unauthorized access affecting data and the computer-generated information and/or automated controls.

Recommendation:
We recommend the MNCR improve/revise the elevated user access provisioning process and control over privileged-level access in the information systems.

Financial Statement Impact:
No Impact

Management Response:
Members in the elevated groups are admins/test accounts of the AD admins group. We are in process of transitioning to both a centralized domain administration as well as a role based delegation with extending DELL Active Roll Server. After we transition to the MTA wide consolidated, centralized Forest/domain Administration, there will not be any other accounts added to the elevated groups and those will then be delegated via Dell Active Role server.
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, 2013, that we wish to bring to your attention:

1. Farebox Revenue Allocation

Observation:
The Farebox revenue allocation between MTA Bus and New York City Transit Authority (“NYCTA”) is not performed on a regular basis.

Background:
MTA Bus Farebox revenue is collected and calculated by NYCTA. Each weekday (weekend days reported on Tuesdays), NYCTA provides a farebox cash revenue report to MTA Bus and Metro Card Revenue on a weekly basis, which details total farebox revenue collected by NYCTA on behalf of MTA Bus. The farebox revenue collected daily is deposited into the MTA Bus Revenue bank account and Metro Card revenue is wired weekly. The Deputy Controller of MTA Bus verifies that the daily deposits for cash revenue and weekly wires for Metro Card Revenue agree to the reported amounts.

Recommendation:
MTA Bus Management should obtain an understanding of the Revenue calculations performed by NYCTA and based on Cubic report perform a recalculation process based on the number of trips and agreed upon rates to recalculate Farebox revenue to ensure that monthly Farebox revenue is appropriate.

Management’s Response (2012):
The formula used to determine the revenue distribution was reviewed and approved by MTA Bus management. In addition, a quarterly review of the data is done by NYCTA and any resulting adjustments processed. Per the recommendation, management will on an annual basis, perform a detailed analysis of a statistical random sample to test the validity of the formula results.

Status Update (2013):
This recommendation is considered partially completed, as MTA Bus is still in the process of working with the New York City Transit Authority to develop a process to test random sampling of revenue data.

Management Response (2013):
MTA Bus management, will on an annual basis, perform a detailed analysis of a statistical random sample to test the validity of the formula results.

Status Update (2014):
This recommendation is considered partially completed, as MTA Bus is still in the process of working with the New York City Transit Authority to develop a process to test random sampling of revenue data.
1. Farebox Revenue Allocation (continued)

*Management Response (2014):*
MTA Bus will conduct a statistical sample of Metro Card swipes during 2015 that will track physical swipes to revenue received. This will be tested against the agreed formula used by NYC Transit to remit fare box revenue to MTA Bus.
NEW YORK CITY TRANSIT AUTHORITY
CURRENT YEAR COMMENTS-DEFICIENCIES-2014

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, 2014, that we wish to bring to your attention:

1. Liability – Time-Based Farecards

Criteria:
Current pronouncements issued by the GASB regarding recognition and measurement of certain liabilities and expenditures in governmental fund financial statements and revenue recognition.

NYCTA management must determine the portion of unearned revenue related to time-based farecards.

Condition:
NYCTA management determines the classification between unearned revenue and earned revenue at month-end based on:

1) First swipes, which trigger revenue recognition
2) The life span of each type of farecard (7 day unlimited, 30 day unlimited, etc.)
3) Cut-off date (month-end or year-end)

At first swipe, all of the revenue associated with a farecard is classified as farecard revenue. At month-end, management must determine a percentage to reclassify to unearned revenue because the life span of the farecard overlaps into the subsequent month. During 2014 and years prior, management estimated the unearned portion based on how many days are on either side of the cut-off date. Further for 7 day cards, management assigned a weighted coefficient to each day of the week in order to reflect actual historical usage.

The AFC Farecard Data Report is a schedule that notes the closing amount based on activity throughout the month (sales, usages, expired, etc.). NYCTA records Time-Based Farecard Liability based on the amount of time-based revenue which overlaps the following month. Any farecard with a time usage period overlapping two months creates a liability (unearned revenue) for the days after month-end. Certain class codes are designated for weekly or monthly Time-Based Farecards. NYCTA uses a weighted coefficient for the last 7 days (for a weekly card) to determine which cards first used in one month will actually generate revenue in the following month. A coefficient is required for accurate reporting of liability since the AFC system recognizes all revenue in each time-based farecard on its first use.

Cause:
NYCTA management does not equally weight weekends and weekdays. The underlying assumption is that the actual usage for that card would be higher during weekdays than it would during the weekend. As a result, the NYCTA would have shifted more of the revenue allocation to the unredeemed liability instead of keeping it as earned revenue.

Revenue should be earned based on a straight-line amortization method over the life span of the farecard.
1. Liability – Time-Based Farecards (continued)

Effect:
In the current year, there were no material differences between the weighted calculation and the straight-line calculation. However, as time-based farecards gain popularity, this could become material in the future.

Recommendation:
NYCTA management should recognize revenue on a straight-line basis over the life-span of the card for all time-based farecards.

Financial Statement Impact:
No material impact

Management Response:
Management concurs. NYCTA will determine earned and unearned revenue on seven day time-based farecards on a straight line basis rather than recognizing unearned revenue based on a weighted average based on usage.

Target date: 2nd Quarter 2015
2. Data Center Access

Criteria:
Physical access to computer areas is limited to authorized IT personnel via a card entry system. Physical access restrictions are in place to provide reasonable assurance that only authorized individuals can gain access to information resources.

Condition:
An excessive number of users have been granted access to the 2 Broadway and 130 Livingston Plaza Data Centers.

Cause:
There are over 500 users with access to each of the Data Centers. Such volume increases the risk of inappropriate access to the Data Center.

Effect:
Individuals gain inappropriate access to equipment in the data center and exploit access to circumvent logical access controls and gain inappropriate access to systems.

Recommendation:
Establish procedures and controls around granting Data Center access as well as the timely review and removal of users’ access that does not align with their day-to-day job responsibilities.

Financial Statement Impact:
No Impact

Management Response:
Management concurs. A procedure has been developed and implemented. Controls are in place for manual review and to remove user access; full automatic controls with annual recertification will be implemented after IAM implements a workflow system for data center access request.

Target date: Implemented
3. Administrative Access

Criteria:
The ability to administer application, DataBase, underlying servers, and domain system security is restricted
to appropriate personnel.

Condition:
Users have privileges beyond those necessary to perform their job responsibilities.

Cause:
The MTA performed an upgrade of the windows operating system, and members of the Operations Server
Administration Group were provided administrator access to perform the system upgrades. Upon the
completion of the upgrade, users’ access privileges were not rescinded and such users maintained access for a
longer period of time than needed.

Effect:
Users have access privileges beyond those necessary to perform their assigned duties, which may create
improper segregation of duties.

Recommendation:
Establish procedures to ensure the timely review and removal of users’ access that does not align with their
day-to-day job responsibilities.

Financial Statement Impact:
No Impact

Management Response (2013):
Management concurs. Access privileges are granted to a discreet population within the Server Operations
Administration Group to facilitate day-to-day responsibilities, including operating system upgrades. These
rights are unique to their daily job function. MTA-IT will continue to monitor user rights to ensure
coordination with job functions.

Target Dates: Implemented.

Status Update (2014):
The identified observation still remains open as of December 31, 2014.

We reiterate our prior recommendation above. In addition, we recommend that MTA BSC establish
procedures to monitor the progress and completion of such reviews to ensure all reviews are adequate.

Management Response (2014):
Management concurs. In 2015, MTA IT infrastructure removed domain admin rights from seven operation
team members on the NYCT active directory. Further, we are in the process of procuring a Privilege Identity
Management System (PIMS) and expect implementation in 2016. MTA BSC DBA accounts have been
recertified in June 2015.

Target Date: Recertification of DBA accounts- 2nd Quarter 2015; Implementation of PIMS- 3rd Quarter 2016
NEW YORK CITY TRANSIT AUTHORITY
PRIOR YEAR COMMENTS - DEFICIENCIES - 2013

4. Security Events Logging

Criteria:
Information security tools over application systems are administrated and implemented to record and report security events (such as security violation reports, unauthorized attempts to access information resources); reports generated are regularly reviewed and necessary action is taken.

Condition:
Active Directory Security Events are not generated and reviewed on a periodic basis.

Cause:
Active Directory Security Events are not generated and reviewed on a periodic basis.

Effect:
Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.

Recommendation:
We recommend that NYCTA enable the system to track security events. In addition, management should establish procedures for the periodic review of security logs to ensure unauthorized events are captured and resolved in timely fashion.

Financial Statement Impact:
No Impact

Management Response (2013):
Management concurs. MTA-IT will work to enable a system to track security events. Further, efforts are currently underway to implement a system to review security logs periodically to ensure the timely capture and resolution of such events.

Target Date: First Quarter 2015.

Status Update (2014):
This comment has not been corrected and remains open.

NYCTA did not log and track security events that occur within the application during 2014. This increases the risk of unauthorized access affecting data and the computer-generated information and/or automated controls.

We reiterate our prior recommendation.

Management's Response (2014):
Management concurs. MTA IT Security has implemented the Security Incidents and Events Management tool (SIEM) which collects data from the Active Directory and is regularly monitored by MTA Cyber Security Operation’s Team.

Target Date: Implemented
OTHER MATTERS

Other matters related to our observations concerning operations, compliance with laws and regulations, and best practices involving internal control over financial reporting that we wish to bring to your attention are as follows:

5. Cash – Revenue Fund Account

Criteria:
Cash accounts are routinely reconciled to supporting documentation. A checklist of all accounts is maintained to validate that all accounts have been reconciled, reviewed, and approved according to NYCTA policy. Reconciling items are investigated timely and adjustments are recorded as necessary.

Condition:
The Revenue Fund Account relates to coins in the machines, funds from the money room, and money from the transit booths.

Cause:
The Revenue Fund Account (G/L 102201) had a recorded balance at December 31, 2014, of $30,680,986. The Undeposited Passenger Revenue Receipts Schedule comprises all sub-schedules that make up the amount in the Revenue Fund Account. The grand total of the schedule, in addition to any reclassifications out of the Cash Clearing Account #231010 into the Revenue Fund Account, should agree to the total in the Revenue Fund Account. The Undeposited Passenger Revenue Receipts Schedule for December 2014 was $35,087,727, less the reclass from the cash clearing account of $3,302,743 equaled $31,784,984.

Effect:
The total amount of the Revenue Fund Account does not reconcile to the Undeposited Passenger Revenue Receipts Schedule. There is a $1,103,998 difference between the general ledger and the schedule.

Recommendation:
Management should review the $1,103,998 reconciling item to determine the nature and cause. Upon completion, an adjustment to the schedule or general ledger should be made.

Financial Statement Impact:
No material impact

Management Response:
Management concurs. The reconciling item noted relates to 2010 activity and is an entry made by Treasury which remained misposted. Subsequent activity has been reconciled to year end 2014. Efforts to isolate the difference will continue and adjustments will be made to the account as required by the third quarter of 2015.

Target Date: Third Quarter 2015
6. Unapplied Cash – A/R

Criteria:
General ledger (G/L) account 161214, Unapplied Cash, is recorded as part of Other Receivables and bears a debit balance at December 31, 2014. An unapplied cash account, when used in order to track cash receipts that cannot immediately be matched to a specific customer, should maintain a credit balance under normal circumstances (dr. cash, cr. unapplied cash).

Condition:
NYCTA utilizes the unapplied cash GL account for the purpose stated above – to record cash receipts in a timely fashion when the customer providing the funds isunknown at that specific point in time. The account maintained approximately a $1.4M debit balance at December 31, 2014. The NYCTA could not explain why the balance was a debit at year-end and/or explain how they arrived at the $1.4M amount.

Cause:
GL account 161214 is not appropriately reconciled or analyzed throughout the year by the NYCTA’s Accounting Department, Treasury Department, or Accounts Receivable Department (MTA BSC). There is a lack of timely and effective communication between the three departments in order to properly monitor the selected GL account.

Effect:
GL account 161214, and “Other Receivables” may be misclassified at year-end.

Note: The effect relates to the classification of Cash and Accounts Receivable. There is no revenue effect.

Recommendation:
Management should implement a structured account analysis to reconcile this account on a periodic basis. Open communication between accounting, treasury, and the MTA BSC would be helpful to understand the timing and nature of cash receipts and the corresponding customer A/R accounts.

Financial Statement Impact:
No Impact

Management Response:
Management concurs. The debit balance originates from the 2011 BSC conversion year. MTA Treasury, NYCT Operations Accounting and BSC Accounts Receivable will continue to research the discrepancy by matching cash applications to the accounts receivable line entries, and adjust the account as required by year end.

Target Date: 4th Quarter 2015
DEFICIENCIES

We identified, and have included below, deficiencies involving the Staten Island Rapid Transit Operating Authority’s (“SIRTOA”) internal control over financial reporting as of December 31, 2014, that we wish to bring to your attention:

1. Inventory Reserve for Obsolescence

Criteria:
GASB Codification- Section I40, Inventory, states the following:

A departure from the cost basis of pricing the inventory is required when the utility of the goods is no longer as great as its cost. A loss should be recognized and accounted for in the current period whenever the utility of goods is impaired by damage, deterioration, obsolescence, changes in price levels, or other causes. Such losses should be measured by applying the method of pricing inventories at cost or market, whichever is lower.

Condition:
The SIRTOA inventory reserve for obsolescence is determined by applying 25% to total inventory at December 31st. This percentage is calculated by taking the New York City Transit Authority (NYCTA) inventory reserve for obsolescence compared to total NYCTA inventory. The NYCTA inventory reserve for obsolescence is methodically calculated within the CMS system through a number of steps. There is no correlation between SIRTOA’s inventory and reserve for obsolescence and NYCTA’s inventory and reserve for obsolescence.

Cause:
SIRTOA does not have a SIRTOA specific process or methodology to determine the inventory reserve for obsolescence.

Effect:
SIRTOA relies on a percentage calculated by NYCTA to determine SIRTOA’s inventory reserve for obsolescence.

Recommendation:
SIRTOA management should develop a SIRTOA specific process for determining the inventory obsolescence reserve. Management should utilize the data provided by the inventory system (TALON) to determine trends and project excess/obsolete inventory.

Financial Statement Impact:
No Impact

Management Response:
Management concurs. Representatives from SIRTOA will work with NYCT Supply Logistics to develop an inventory obsolescence methodology consistent with the operating requirements of SIRTOA.

Target Date: 4th Quarter 2015
DEFIENCIES

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, 2014, that we wish to bring to your attention:

1. Classification of Liabilities

Criteria:
Accounting staff prepare all journal entries for the Accounting Manager’s review, approval and sign-off. In the absence of the Accounting Manager, the Assistant Accounting Manager reviews, approves, and signs-off on all journal entries. In addition, the Assistant Controller and Controller review, approve, and sign-off on all journal entries.

Condition:
Upon receipt by the TBTA of the New York City Employee Retirement System pension contribution invoice for $32,109,883 an incorrect credit was made to account #208234- Due to Outside Vendors.

Cause:
Management did not properly review the journal entry and supporting documentation prior to posting the journal entry in the PeopleSoft accounting system.

Effect:
As a result, $32,109,883 was erroneously recorded in general ledger account #208234- Due to Outside Vendors when it should have been recorded to general ledger account #206305- Pension Contribution Withheld. Based on an audit commendation, this was corrected by management prior to closing the general ledger for 2014.

Recommendation:
Management should thoroughly review all journal entries and supporting documentation to ensure amounts are posted to the correct general ledger account numbers.

Financial Statement Impact:
Reclassification between liability general ledger accounts. Net effect on the liability balance was zero.

Management Response:
Management agrees. All journal entries and supporting documentation will be thoroughly reviewed to assure amounts are posted to the correct general ledger accounts.
2. Data Center Access

Criteria:
Physical access to computer areas is limited to authorized IT personnel via a card entry system. Physical access restrictions are in place to provide reasonable assurance that only authorized individuals can gain access to information resources.

Condition:
An excessive number of users have been granted access to the 2 Broadway and 130 Livingston Plaza Data Centers.

Cause:
There are over 500 users with access to each of the Data Centers. Such volume increases the risk of inappropriate access to the Data Center.

Effect:
Individuals gain inappropriate access to equipment in the data center and exploit such access to circumvent logical access controls and gain access to the systems.

Recommendation:
Establish procedures and controls around granting the Data Center Access as well as the timely review and removal of users’ access that does not align with their day-to-day job responsibilities.

Financial Statement Impact:
No Impact

Management Response:
Data Center Access is now handled by MTA HQ IT Security and Data Center Operation’s divisions. Currently MTA IT is consolidating the policies and procedures and will take the recommendations into consideration and follow the necessary guidelines.
3. Administrative rights to the Kronos Application

Criteria:
The ability to make modifications to overall system security parameters, security roles, or security configuration over network and communication software is limited to appropriate IT personnel.

Condition:
A user was granted administrative rights to the Kronos Application, which was inappropriate based on his job responsibility.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access affecting data and the computer-generated information and/or automated controls.

Recommendation:
We recommend that TBTA management establish procedures to review user access request prior to access being granted to ensure that user requests for elevated access gain such access based on their job responsibility.

Financial Statement Impact:
No Impact

Management Response:
The administrative rights of the user indicated above were immediately changed to “View” only. This recommendation has been implemented. The procedure to obtain access is through the electronic request for Kronos Access that must be approved by the Director of the Central Control Unit.
4. Kronos Application Password Parameters

**Criteria:**
The identity of users is authenticated to the systems software through passwords or other authentication mechanisms, in compliance with entity security policies. The use of passwords incorporates policies on periodic change, confidentiality, and password format (e.g., password length, alphanumeric content, expiration, account lockout).

**Condition:**
The password expiration and password complexity enforced within Kronos is not in compliance with MTA security policy and procedures. Password history is set to 60 days in Kronos, which is not in accordance with TBTA Information Security Policy requiring users to change passwords every 30 days. No password complexity is enforced within Kronos which is not in accordance with TBTA Information Security Policy requiring users to use alphanumeric characters.

**Cause:**
TBTA did not follow security policies and procedures guidelines.

**Effect:**
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access affecting data and the computer-generated information and/or automated controls.

**Recommendation:**
We recommend that TBTA align their password parameters with security policies and procedures guidelines.

**Financial Statement Impact:**
No Impact

**Management Response (2013):**
We have enforced the password complexity according to MTA Midrange Information Systems Security policy directive and feel no further strengthening is necessary. We have chosen to have 60 days mandatory password change option to avoid frequent account lockouts and password resets. We feel we have adequate user controls to avoid 30 day password expiration. As stated in our response to your follow up of 2012 Letter of Recommendations, we can consider changing the expiry to 30 days with the implementation of a future Identity Management system. We believe, without password synchronization or a single sign-on authentication, having multiple passwords that expire in 30 days will be counterproductive to our user departments and also will cause help-desk support calls to increase.

**Status Update (2014):**
This comment has not been corrected and remains open.

We reiterate our prior recommendation that MTA TBTA align their password parameters with security policies and procedures guidelines.
4. Kronos Application Password Parameters (continued)

*Management Response (2014):*
MTA IT Enterprise Application support will meet with IT security to review security policies and procedures to ensure proper security measures in Kronos Workforce Central. We expect to fully implement by October 1, 2015.
5. Oracle Database Password Parameters

Criteria:
The identity of users is authenticated to the systems software through passwords or other authentication mechanisms, in compliance with entity security policies. The use of passwords incorporates policies on periodic change, confidentiality, and password format (e.g., password length, alphanumeric content, expiration, account lockout).

Condition:
The password expiration enforced within the Oracle Database is not in compliance with MTA security policy and procedures. Password history is set to 60 days in Oracle Database, which is not in accordance with TBTA Information Security Policy requiring users to change passwords every 30 days.

Cause:
TBTA did not follow security policies and procedures guidelines.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases the risk of unauthorized access affecting data and the computer-generated information and/or automated controls.

Recommendation:
We recommend that TBTA align their password parameters with security policies and procedures guidelines.

Financial Statement Impact:
No Impact

Management Response (2013):
Our users do not login to the Oracle Database directly. All the access to the Database is channeled through the Middle Ware. Therefore, this recommendation cannot be implemented in the present Application Architecture.

Status Update (2014):
This comment has not been corrected and remains open.

We reiterate our prior recommendation.

Management Response (2014):
Oracle Database Password Parameters is now handled by MTA HQ IT Enterprise Applications/Database Administration group. This task will be discussed and will take the recommendations into consideration in conjunction with the recommendations under item #4 above and follow the necessary guidelines.
6. Windows Password Parameters

Criteria:
The identity of users is authenticated to the systems software through passwords or other authentication mechanisms, in compliance with entity security policies. The use of passwords incorporates policies on periodic change, confidentiality, and password format (e.g., password length, alphanumeric content, expiration, account lockout).

Condition:
The password expiration, complexity and invalid logon attempts enforced within Windows is not in compliance with MTA security policy and procedures. Account Lockout Threshold is set to 7 invalid logon attempts on the mtabt.org domain which is not in accordance with TBTA Information Security Policy requiring password lockout after 3 invalid attempts. Password history is set to 60 days in Windows which is not in accordance with TBTA Information Security Policy requiring users to change passwords every 30 days. No password complexity is enforced within Kronos which is not in accordance with TBTA Information Security Policy requiring users to use alphanumeric characters.

Cause:
TBTA did not follow security policies and procedures guidelines.

Effect:
Security mechanisms are inadequate, ineffective, or inconsistent due to lack of established security policies and standards. This increases risk of unauthorized access affecting data that underlie computer-generated information and/or automated controls.

Recommendation:
We recommend that TBTA align their password parameters with security policies and procedures guidelines.

Financial Statement Impact:
No Impact

Management Response (2013):
We have enforced the password complexity according to MTA Midrange Information Systems Security policy directive and feel no further strengthening is necessary. We have chosen to have 60 days mandatory password change option to avoid frequent account lockouts and password resets. We feel we have adequate user controls to avoid 30 day password expiration. As stated in our response to your follow up of 2012 Letter of Recommendations, we can consider changing the expiry to 30 days with the implementation of a future Identity Management system. We believe, without password synchronization or a single sign-on authentication, having multiple passwords that expire in 30 days will be counterproductive to our user departments and also will cause help-desk support calls to increase.

Status Update (2014):
This comment has not been corrected and remains open.

We reiterate our prior recommendation that MTA TBTA align their password parameters with security policies and procedures guidelines.
6. Windows Password Parameters (continued)

*Management Response (2014):*
Windows Password Parameters are now managed by MTA HQ IT Infrastructure group. This task will be discussed and will take the recommendations into consideration in conjunction with the recommendations under items #4 and #5 above and follow the necessary guidelines.
7. Job Processing Documentation

Criteria:
Automated scheduling tools have been implemented for the completeness of the flow of processing and are monitored by the Information Technology Department. Access to job scheduling tools is appropriately restricted.

Condition:
We were unable to obtain appropriate documentation around how error was resolved.

Cause:
TBTA did not retain appropriate documentation to show batch job processing failures are appropriately reviewed and resolved.

Effect:
Production systems, programs, and/or jobs result in inaccurate, incomplete, or unauthorized processing of data.

Recommendation:
We recommend that TBTA to monitor batch processing failures and retain documentation around how failures were reviewed and resolved.

Financial Statement Impact:
No Impact

Management Response (2013):
Agree. We do not keep documentation of how the failures have been reviewed and resolved although such evidence can be gathered from the email system and/or from the log of the help-desk trouble tickets if necessary. Electronic records of the status of all batch processing jobs are available on line through Kronos Transaction Assistant Screen based upon a start date and an end date. We believe we will be better equipped to fully implement this recommendation after the implementation of a Centralized Help Desk Support Software (Maximo).

Status Update (2014):
This comment has not been corrected and remains open.

We reiterate our prior recommendation that MTA TBTA retain appropriate documentation to show batch job processing failures are appropriately reviewed and resolved.

Management Response (2014):
This recommendation has been implemented. IT application support now monitors daily Kronos and Bio Demo interfaces for errors. Once errors are identified, they are logged in a spreadsheet on the network and then corrected by resubmitting interface.
8. Succession Planning

**Observation:**
This comment has been tailored for the TBTA 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. In addition, many governments face the challenge of offering competitive compensation packages to entice strong candidates to come work for 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.

- **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
8. Succession Planning (continued)

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

- Design of better recruitment and retention practices may aid in the succession process. Making sure pay levels are competitive with the market place is a critical means of retaining employees. Providing career advancement opportunities for employees is another means of retention.

- 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 TBTA 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 TBTA; 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 TBTA needs. In addition TBTA should ensure that competitive compensation packages are in place in order to entice strong, competent, and talented candidates to come work TBTA.

Management Response (2012):
MTA Bridges and Tunnels (legal name Triborough Bridge and Tunnel Authority) concurs with this recommendation and has, or will, take the following actions in 2013.

4) TBTA is identifying mission critical positions that are hard to fill because of the requirements of job or may become vacant due to retirements.

5) TBTA is conducting an age/years-of-service analysis by Department and by individual to project upcoming attritions due to retirements.

6) TBTA is reviewing the structure of several Departments, to create a pipeline of high potential employees to fill critical positions identified in “1” above. This restructuring, to be reviewed with
8. Succession Planning (continued)

MTAHQ as appropriate will facilitate the transfer of knowledge and enable additional employees to
develop high level relationships and authority both within the Agency as well as with relevant
external stakeholders. In another effort to facilitate knowledge transfer, all Departments will begin a
review of their policies and procedures in 2013, updating where necessary.

7) TBTA is reviewing Managerial Position Questionnaires (MPQs) to ensure they are appropriately
evaluated and to ensure that salaries for the positions allow for the attraction and retention of agency
talent.

8) Continue to work with MTA HQ and the Business Service Center on the development of a Talent
Management System that identifies high potential employees not only within the TBTA but within
other MTA entities to fill positions as they are identified. This system will leverage existing
PeopleSoft modules.

9) TBTA has begun a Management Associates Program in which high potential entry level employees,
identified in a competitive process, rotate through five different Departmental assignments in six
month blocks and receive regular management training. At the end of the program, they will compete
for open positions within the Agency.

Status Update (2013):
While some progress has been made to ensure that the proper strategic approach to succession planning at all
levels, including the identification of mission critical positions, has been implemented, focus should continue
in this area. Therefore, we reiterate our 2012 recommendation.

Management Response (2013):
Management agrees and will continue the process of implementing the six initiatives enumerated in the 2012
Management response.

Status Update (2014):
Focus should remain on the identification of mission critical positions for strategic succession planning at all
levels. We reiterate our prior recommendation.

Management Response (2014):
Succession Planning continues to be a critical priority for Senior Management.
9. 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 (2011):
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.

Status Update (2012):
1. There were $206 thousand of unrecorded accrued liabilities related to invoices received subsequent to December 31, 2012 related to services performed prior to December 31, 2012.

2. There were $172 thousand in liabilities that were incorrectly recorded at December 31, 2012.
9. Operating and Capital Accruals (continued)

Management Response (2012):
The Engineering and Controller’s staffs will jointly further strengthen the procedures over the year-end process for estimating capital and operating accruals.

Status Update (2013):
1. There was one invoice for $538,240 recorded twice in accrued liabilities at December 31, 2013.

2. When comparing estimates to actual invoices received, there were $1,946,048 in net liabilities that were incorrectly recorded at December 31, 2013.

Management Response (2013):
Management will institute a procedure at year end, in which estimates are adjusted to invoices received, and differences recorded in the accounts.

Status Update (2014):
1. Bond issue costs were over accrued by $600,000 at December 31, 2014, when compared to actual invoices received subsequent to December 31, 2014.

2. When comparing accrual estimates to actual invoices received, there were $663,265 in capital accruals that were not recorded at December 31, 2014.

Management Response (2014):
Management agrees and will enhance the year-end process of adjusting accruals as invoices are received.
TRIBOROUGH BRIDGE AND TUNNEL AUTHORITY
PRIOR YEAR COMMENTS- DEFICIENCIES- 2011

10. 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 (2011):**
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.

**Status Update (2012):**
This comment has not been corrected and remains open.

**Management’s Response (2012):**
Time keeping function is now re-aligned with Operations Department and being done by a separate unit called CCU. This was created during Kronos implementation to carry out the functions that were previously done by HR. Technology Department has updated the document to reflect the changes in the new Kronos 6.2 system. CCU is working on addressing this recommendation and has agreed to complete by the Third Quarter of 2013.

**Status Update (2013):**
This comment has not been corrected and remains open.

**Management’s Response (2013):**
In 2013 we partially implemented the User Access Re-certification recommendation. These activities completed in 2013 provide us the basis to do a complete annual re-certification in 2014 as recommended. The following activities were completed in 2013:
- Documented Kronos 6.2 Certification Procedure
- Certified that only active and temporarily inactive employees are in Kronos
- Completed data cleansing by removing obsolete Function Access Profiles in the Kronos Database
- Certified Function Access Profiles and linked them to Kronos Licensing for proper assignment.

In 2014, Technology and Central Control Unit (CCU) departments will work together to complete the re-certification process as set forth in the documentation mentioned above.

**Status Update (2014):**
This comment has not been corrected and remains open.
10. User Access Reviews (Kronos) (continued)

Management’s Response (2014):
The certification process will be completed by September 1, 2015.
11. 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 (2011):**
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.

**Status Update (2012):**
This comment has not been corrected and remains open.

**Management’s Response (2012):**
This has been completed. Following parameters have been set in Oracle.
   a) Password Expires in 60 days
   b) Strong Passwords with minimum of 8 characters long. They must be a combination of numbers, special characters and upper and lower case letters.

**Status Update (2013):**
Some progress has been made and password parameters are now enforced at database level. D&T noted that the password parameters enforced are not aligned with MTA security policies and procedures.

**Management’s Response (2013):**
Practice has been to set the password to expire in 60 days. This is true for Network, Database and Application logins throughout the organization. In the absence of a password synchronization or a single sign-on authentication, if the password is to expire in 30 days users will be forced to change the passwords very frequently which will cause user lockouts and password resets to increase tremendously. With the implementation of a future Identity Management system, we can consider changing the expiry to 30 days.

**Status Update (2014):**
Some progress has been made and password parameters are now enforced at database level, however the password parameters that are now enforced are not aligned with MTA security policies and procedures.
11. Database Password Controls (Kronos) (continued)

Management’s Response (2014):
Database Password Controls (Kronos) is now handled by MTA HQ IT Enterprise Applications/Database Administration group. This task will be discussed and will take the recommendations into consideration in conjunction with the recommendations under item #5 above and follow the necessary guide lines.
PRIOR YEAR COMMENTS ADDRESSED
PRIOR YEAR COMMENTS ADDRESSED

Metropolitan Transportation Authority- Headquarters

1. Operating and Capital Accruals- 2013
4. Classification of Long Term Debt – 2013
5. Internal Cash Transfers – 2013
6. Oracle DataBase Password Parameters- 2013

MTA Business Service Center

1. Bank Reconciliations- Maintaining Documentation of Agencies’ Approval- 2012
2. Retrospective Review of Paid and Open Invoices after Year-End- 2011
3. Phire Application Password Parameters- 2013
4. PeopleSoft Application and DataBase Password Parameters- 2013
5. Database Password Controls- 2011

First Mutual Transportation Assurance Company

1. Formally Documenting the Risk Assessment Process – 2013

Long Island Rail Road Company

None

MTA Bus Company

None

New York City Transit Authority

1. Processing Healthcare Claims- 2013

Staten Island Rapid Transit Operating Authority

1. Compliance with National Transit Database Reporting- 2013

Triborough Bridge and Tunnel Authority

1. Classification of Receivables- 2013
DEFINITIONS

The definitions of a deficiency, a material weakness, and a significant deficiency are as follows:

A deficiency in internal control over financial reporting 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.

A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity’s financial statements will not be prevented, or detected and corrected on a timely basis.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.