

New York City Transit Authority

**Management Letter Comments
December 31, 2007**

April 28, 2008

Dear Audit Committee Members:

In planning and performing our audit of the consolidated financial statements of New York City Transit Authority (the "Authority") as of and for the year ended December 31, 2007, in accordance with auditing standards generally accepted in the United States of America, we considered its internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the Authority's internal control over financial reporting. Accordingly, we do not express an opinion on the Authority's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses as defined in the recent amendment to AU 325, *Communicating Internal Control Related Matters Identified in an Audit*, of the AICPA Professional Standards and shown below:

Control deficiency – exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Significant deficiency - a control deficiency, or combination of control deficiencies, that adversely affects the company's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected.

Material weakness - a control deficiency, or combination of control deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

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

If you would like any further information or would like to discuss any of the issues raised, please contact Mike Hayes at (203) 539-5713.

Very truly yours,



**New York City Transit Authority
2007 Financial Audit
Management Letter Comments**

1.	Standardize Change Management Process Across All Financially Significant Applications ..	2
2.	Strengthen EIS Security	4
3.	Enhance User Access Provisioning Procedures and User Access Removal Procedures for Terminated Employees.....	5
4.	Expand Periodic Reviews Over Access	6
5.	Strengthen Unix Security	7
6.	Strengthen Password Controls on Mainframe and Review of Mainframe Violation Reports ...	8
7.	Minimize Use of Shared IDs in ATS	10
8.	Strengthen AS400 Security.....	11
9.	Strengthen Oracle DB Security	12
10.	Enforce Segregation of Duties Over Access to the Test and Production Environments	14

Items 1 through 9 are recurring comments from our 2006 Management Letter.

New York City Transit Authority

2007 Financial Audit

Management Letter Comments

I. Internal Control Observations – 2007 Audit

1. Standardize Change Management Process Across All Financially Significant Applications

Observation:

Each financially significant application has its own separate process for managing changes to the application. Our testing identified the following:

- For non-mainframe changes, there is no report from either a version control library or a production library to provide the system generated full population for all changes moved into production.
- Formal User Acceptance Testing and user sign-off were not consistently performed before the changes were submitted for migration into the production environment.
- There is no formal QA function to ensure the compliance of the process across all the applications, and a separate migration group has not been applied to all of the non-Mainframe applications.
- Manager approval was not consistently obtained before changes were migrated into the production environment.
- Evidence of IT testing was not always provided.
- Segregation of Duties issues are noted in some applications where developers have access to both changing the code and promoting it to production.

Implication:

The lack of strong processes and controls to manage changes to financially significant applications increases the risk that unauthorized changes are made to the application. The lack of such controls also increases the risk that changes are inadequately tested before migration to the production environment. This may introduce inadvertent changes to the application that impact the processing of live business transactions; potentially affecting the integrity and accuracy of the financial statements.

Recommendation:

We recommend that management implement standardized processes and controls throughout New York City Transit for all changes that are made to applications that can have an effect on the financial statements (e.g., AFC, PRAS, G/L, Kronos, Payroll, EIS, UTS, & ATS). The following points should be considered in the controls:

- Use of standard request forms for both external (user group) & internal (TIS group) requests.
- All requests should be tracked, monitored and approved appropriately by either the user group (for user requests) or by the respective TIS group manager.
- User testing, as well as programmer testing, should be implemented for all changes and should include formally documented approval. In the case that user testing is deemed unnecessary, a formal waiver should be obtained from the user group for each case.
- The responsibilities for developing the changes and moving the changes into the live production environment should be segregated (e.g., the people who code the changes should not have access to move changes to production and vice versa).
- A quality assurance function should be implemented to ensure that all of the requirements above are met prior to moving the changes to the production environment.

**New York City Transit Authority
2007 Financial Audit
Management Letter Comments**

Management Response:

Management concurs. Standardization of the Change Management/QA functions across all financially significant applications has been approved and funded in the 2008 budget. Because this process involves several major applications, implementation will be conducted in a phased manner and is expected to be completed in 2010.

Target Dates:

- Phase I: Procuring resources, training, and developing systematic change management procedures – 1st quarter, 2008.
- Phase II: Process implementation for limited critical applications – 4th quarter, 2008.
- Phase III: Review results and develop a roll out plan for all financially significant applications – 2nd quarter, 2009.
- Phase IV: Deploy to remaining financially significant applications – 4th quarter, 2010.

New York City Transit Authority

2007 Financial Audit

Management Letter Comments

2. Strengthen EIS Security

Observation:

Review of the EIS system configuration identified the following:

- There is no password complexity (parameter for having both alpha and numeric characters) required.
- During our review, there were 22 super users noted in the system. Many of these users are members of the TIS EIS team that HR has deemed appropriate users of the system.
- Obtained a periodic recertification of 2006 users which was completed in third quarter, 2007.
- During the engagement, monitoring controls had not yet been implemented.

Implication:

Lack of adequate password settings and the existence of users having sensitive access increase the risk of unauthorized access to the system. Without adequate monitoring controls in place, this also increases the risk that unauthorized or inadvertent changes made to EIS standing data go undetected and uncorrected.

Recommendation:

We recommend that management consider the following options:

- Utilize the full breadth of password controls provided by the system to improve EIS security.
- Consider the reduction of individuals that have sensitive and super user access to the system.
- Recertification of users should be performed in a more relevant time frame, closer to the point in time.
- Implement monitoring controls to detect and prevent unauthorized or inadvertent changes to the system.

Management Response:

Management concurs.

- Dependent upon installation of Identity Management System (IVAULT).
- Super Users will be reduced from 22 to 11 with proper functional justification.
- TIS will continue to work with Human Resources to schedule and recertify all EIS users in a timely manner.
- Automated monitoring controls: Implemented 1st quarter, 2008.

Target Dates:

- Password controls - 2nd quarter, 2008.
- Super user access - 1st quarter, 2008.
- Recertification of users - Ongoing annually.

**New York City Transit Authority
2007 Financial Audit
Management Letter Comments**

3. Enhance User Access Provisioning Procedures and User Access Removal Procedures for Terminated Employees

Observation:

- (1) In response to our comment from the prior year, Management has implemented a new user provisioning set of polices and procedures for ATS and Kronos. However, our review of user access provisioning noted that several users were not consistently approved prior to the creation of the user ID over several applications (AS400,RRS, UTS, and Kronos).
- (2) Our review of user terminations noted that some users still had access to financially significant systems even though they had been terminated. These environments included the AS400, RRS, UTS, and Kronos.

Implication:

- (1) Deviation from the proper procedure and controls on setting up user access increases the risk of unauthorized and inappropriate access to financially significant applications, and may compromise the integrity of the data for such applications.
- (2) There is an increased risk of unauthorized access to the systems when user accounts for employees who no longer work for New York City Transit are still enabled.

Recommendation:

- (1) We recommend that management reinforce compliance over granting user access to ensure that users are given access only upon proper approval and based on job responsibility.
- (2) We recommend that the processes to revoke/disable the access of all terminated employees in a timely manner be improved and followed consistently.

Management Response:

- (1) Management concurs. All affected areas will be reinstructed on the Application Access Control Procedure issued by TIS IS&C in 2007. Where possible, Applications will transfer the responsibility of creating and revoking access to TIS Security.
- (2) Management Concurs. User access removal procedures are ultimately addressed with the full implementation of the I-Vault initiative. In the interim, a monthly report is run to identify terminated employees and deactivate their IDs on EIS. AFC & RRS have deactivated terminated employee IDs and annual reconciliations are performed. The Kronos/I-Vault interface has also been delayed until the implementation of the Identity Management System (IVAULT).

Target Dates:

- (1) User Access Control procedures - 3rd quarter, 2008.
- (2) Access removal for terminated employees - 1st quarter, 2008.

**New York City Transit Authority
2007 Financial Audit
Management Letter Comments**

4. Expand Periodic Reviews Over Access

Observation:

For the AS400, there are no periodic reviews of operating system parameters to ensure they remain appropriate and adequate over time. Also, there is no evidence that periodic reviews of user access are performed for ATS, UTS, and Kronos.

Implication:

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

Recommendation:

We recommend that management perform periodic reviews throughout the year to ensure that all system parameters and employee access are appropriate and adequate over time.

Management Response:

For the AS400, Livingston Plaza Data Center performs a monthly review of operating system parameters on its IBM AS/400, IBM RS/6000, Hewlett Packard HP/9000, and Hewlett Packard SuperDome computer systems. E-Mails from the technicians performing these reviews are sent to the Manager of Technical Support stating that the monthly review has been performed and explicitly stating either that parameter settings were found to be appropriate, or that specific parameter settings should be changed. For parameters flagged as candidates to be reset, the Manager of Technical Support will:

- 1) Determine the appropriateness of changes to parameters;
- 2) Coordinate any potential parameter changes with all affected parties, including the vendors of the systems in question;
- 3) Initiate Change Management for any changes that have been designated as appropriate and safe; and
- 4) Ensure that parameters have been re-set according to plan.

For ATS, UTS and Kronos, all Application owners will be reinstructed regarding the Applications Access Control Procedure issued 2/10/07.

Target Date:

3rd quarter, 2008.

**New York City Transit Authority
2007 Financial Audit
Management Letter Comments**

5. Strengthen Unix Security

Observation:

There are a number of security vulnerabilities on the Unix operating system that supports the EIS Application (PeopleSoft Human Resources) and UTS (Universal Timekeeping System).

Implication:

A weakness in operating system security diminishes the strength of user authentication for individuals accessing the Unix server, which increases the risk of unauthorized access to the server and the applications that reside on that platform (EIS PeopleSoft HR and UTS). These vulnerabilities could be exploited to gain unauthorized access to sensitive information or to deny use of the respective applications.

Recommendation:

We recommend that management address the security issues communicated during the 2007 audit related to the Unix server supporting the EIS application. Upon management assessment, changes should be applied to other Unix servers, as applicable.

Management Response:

Management concurs. TIS Data Center Management will implement action plans to address the vulnerabilities noted, wherever feasible.

Target Date:

2nd quarter, 2008.

New York City Transit Authority

2007 Financial Audit

Management Letter Comments

6. Strengthen Password Controls on Mainframe and Review of Mainframe Violation Reports

Observation:

(1) We noted various weaknesses in password parameters in the following environments: AS400, Unix, ATS (Timekeeping), UTS, Kronos. Examples of these are as follows:

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

(2) Mainframe violation reports were not able to be matched to all of the corresponding emails to obtain authorization for the violations that occurred that day. Also, there were instances when no violation emails were obtained for the day selected. There is discussion to try to automate the distribution of the mainframe violation reports to each of the managers.

Implication:

(1) The lack of strong password controls (e.g., password expiration, minimum length, etc.) increases the risk of unauthorized access to systems.

(2) Unauthorized access attempts to the mainframe could go undetected.

Recommendation:

(1) We recommend that management consider the following options by applying a risk based approach for each application:

- Harden password controls for the specific over applications and systems listed above according to the risks identified in Management's risk based approach that allow for more complex password configurations.
- Implement compensating controls (such as monitoring of certain transactions) to mitigate the inherent risks caused by system limitations.

(2) Implement the automated control in a timely manner so that the violation notifications can be sent to the appropriate managers without manual distribution, thereby reducing the chance of the control not being performed.

Management Response:

(1) Management concurs

- TIS Applications, in conjunction with the respective System Owners, will evaluate and where possible implement appropriate complex password configuration requirements and/or monitoring controls.
- ATS will modify its main logon screen to add a userid field for authentication. The delay is attributed to rejection of a proposed modification and IS&C has now enlisted Tech Support to develop a new screen. Kronos is working with IS&C on implementing an I-Vault interface which will handle all user ID security issues (setup/resets/authentication). Similarly UTS will handle its security issues via I-Vault as well. In the interim, the application will be upgraded to Oracle database version 10g to insure password expiration and user lock out works properly. The expected completion date of the upgrade is 2nd quarter of 2008

New York City Transit Authority
2007 Financial Audit
Management Letter Comments

(2) Management concurs. The feasibility of automating violation notifications is still being evaluated with the software vendor.

Target Dates:

(1)

- Password complexity - 2nd quarter, 2008.
- ATS - 3rd quarter, 2008 and c) Kronos - 1st quarter, 2008.

(2) 2nd quarter, 2008.

**New York City Transit Authority
2007 Financial Audit
Management Letter Comments**

7. Minimize Use of Shared IDs in ATS

Observation:

ATS (Timekeeping) access is gained through AS400 access with shared IDs. Each department has their own shared ID. Since these IDs are shared, termination of a single user does not trigger the removal of the shared ID since the ID is still used by others in the department.

Implication:

The lack of appropriate auditing, authorization, accountability, and authentication with the use of shared IDs increases the risk of unauthorized access to the system. For example, a terminated employee with knowledge of the password has the ability to do something untoward in the system.

Recommendation:

Each employee should be granted his or her own AS400 ID to gain access to the ATS application so that all transactions that take place in the system can be accurately traced to the individual who performed them. In addition, the use of individual user IDs allows the removal of that access should the user be terminated.

Management Response:

Management concurs. AS/400 - TIS Security in conjunction with TIS Applications is working to implement a system that will enable the granting and removal of individual ID's to employees.

Target Date:

3rd quarter, 2008.

**New York City Transit Authority
2007 Financial Audit
Management Letter Comments**

8. Strengthen AS400 Security

Observation:

A number of configured settings on the AS400 supporting ATS (Timekeeping) could be configured to strengthen security.

Implication:

A weakness in operating system security diminishes the strength of user authentication for individuals accessing the AS400, which increases the risk of unauthorized access to the server and the application (ATS) that resides on that platform.

Recommendation:

We recommend that, at a minimum, management analyze the current settings for some of the more critical parameters identified and determine the feasibility of changing the settings to strengthen the security on the AS400.

Management Response:

Management concurs. Where feasible, configuration setting changes have been implemented. A value of *CHANGE can not be implemented globally due to AS400 application's use of temporary files in their application programs. *USE or *EXCLUDE would not allow application program to operate on the files.

The value "1" is necessary for LPDC Technical Support and TIS Security to perform their respective functions, which may require concurrent sign-on.

Target Date:

Completed 1st quarter, 2008.

New York City Transit Authority

2007 Financial Audit

Management Letter Comments

9. Strengthen Oracle DB Security

Observation:

We noted a number of security vulnerabilities on the Oracle database which supports the UTS and EIS applications.

- Generic IDs (such as SYS and SYSTEM accounts) could be used by DBAs to perform database maintenance.
- There also may not be any means of determining if any of the application accounts (accounts with 2 as part of the account name) are being used to attempt to gain access to the database server and tables. System integrity could be comprised if the operating system cannot identify each username's role.
- The following password management controls are not in place: new users are not required to change their password at first login; passwords are only required to be at least 4 characters long; passwords are not locked after successive failed login attempts; accounts are not restricted to single concurrent login; and accounts do not time out after a period of inactivity.

Implication:

Without auditing important Oracle parameters such as sensitive or critical objects and events, security violations can occur undetected for prolonged periods of time and the re-creation of prior events is difficult. There is an increased risk of unauthorized users gaining access to the system and their actions being unrecorded or untraceable.

In addition, the lack of strong password controls increases the risk of unauthorized access to systems.

Recommendation:

We recommend that management consider the following options:

- An independent party should perform the review of the generic IDs (such as SYS and SYSTEM accounts) as well as the DBA activity.
- Accounts should be configured to allow the operating system to manage the role grants for all database usernames.
- Improve password controls over applications and systems that allow for more complex password configurations and implement compensating controls (such as monitoring of certain transactions) to mitigate the inherent risks caused by system limitations.

Management Response:

Management concurs:

- In UTS database, SYS and SYSTEM user ids have very strong passwords and are being used only on as needed basis such as an upgrade to new release/patch or installing new system packages/procedures. All Enterprise DBAs use their own ids to perform their daily tasks.
- The UTS Applications account has limited DBA privileges. The account can not adjust any UNIX resource. The UTS Applications account is the owner of the schema (all the tables, triggers and packages for the application). The default passwords for the EIS SYS and SYSTEM oracle ids are changed periodically and locked away by the enterprise DBA. The PeopleSoft Application software requires the use of a delivered system administration id to perform maintenance and upgrades to the database. As such, the UTS Applications account and PeopleSoft system administration ids are the

New York City Transit Authority
2007 Financial Audit
Management Letter Comments

only ids that can install and modify tables, triggers and packages in the EIS and UTS production environments.

- Improved password controls and procedures will be addressed with the full implementation of the I-Vault initiative, 1Q09. A Corporate DBA policy will be developed that governs Oracle DBA security.

Target Date:
2nd quarter, 2008.

New York City Transit Authority
2007 Financial Audit
Management Letter Comments

10. Enforce Segregation of Duties Over Access to the Test and Production Environments

Observation:

One UTS developer had inappropriate access to both the development and production environments. Observed that Management took immediate action and limited the developer's access to read-only access in the production environment.

Also, noted a Segregation of Duties issue in the RRS application. While Management restricted the sole developer's access to the production environment, the developer also has access to the generic DBA ID which has access to the production environment.

Implication:

Lack of segregation of duties could result in unauthorized and inappropriate changes to the application.

Recommendation:

Ensure appropriate segregation of duties exist for developers; restrict developer's access to the production environment.

Management's response:

Management concurs. UTS procedures have been modified to ensure the appropriate segregation of duties and access restriction controls are addressed.

Target Date:

Implemented – 1st quarter, 2008.