

Deloitte

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

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

March 24, 2008

The Audit Committee
Metropolitan Transportation Authority
New York, New York

And

The Management of Metro-North Commuter Railroad Company
New York, New York

Dear Members of the Audit Committee and Management:

In planning and performing our audit of the financial statements of Metro-North Commuter Railroad Company (the "Company"), a wholly owned public benefit corporation subsidiary of Metropolitan Transportation Authority ("MTA"), as of and for the year ended December 31, 2007 (on which we have issued our report dated March 24, 2008), which contains an explanatory paragraph regarding the adoption of Governmental Accounting Standards Board Statement (GASB) No. 45, *Accounting and Financial Reporting by Employers for Post Employment benefits Other Than Pensions*, in accordance with auditing standards generally accepted in the United States of America, we considered the Company'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 Company's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Company's internal control over financial reporting.

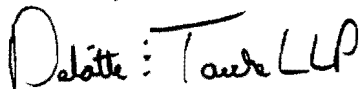
Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting. However, in connection with our audit, we identified, and included in the attached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

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

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

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

Yours truly,



SECTION I – OTHER CONTROL DEFICIENCIES

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

1. PeopleSoft Application Security

Observation:

Application security for the PeopleSoft environment can be strengthened.

Background:

During the course of 2007, Metro-North had several PeopleSoft consultants on the property performing upgrades of the Metro-North PeopleSoft environment. During these upgrades it is not unusual for the consultants to extract data from the live environment, perform modifications in a staging environment, and then reload the data back into the live environment. This sometimes causes incorrect security assignments that were made by the consultants during testing, to be carried over into the live environment. It is Metro North’s standard practice to spend the time necessary after an upgrade, to identify any potential security problems that may have been caused by the upgrade. However, this process could not be done by Metro-North before we began our year end audit and hence there were some “housekeeping” issues that needed to be taken care of.

PeopleSoft HR:

- There are 186 user accounts that remained active in the system even though the users were terminated.
- 9 users were assigned permission MNR_HLPDSK_PSWD_C which allows them to reset passwords. This permission is not required as part of their job function.

PeopleSoft Financials:

- There are 12 user accounts that remained active in the system even though the users were terminated.
- One user has access to certain critical permissions in PeopleSoft Financials. This user does not require access to these permissions as part of his job function.

Recommendation:

PeopleSoft HR:

- Management should consider disabling or deleting the user ids for terminated users in PeopleSoft HR to prevent unauthorized access within the system to maintain consistency in the cleanup efforts as within the PeopleSoft Enterprise Portal.
- Management should consider removing the rights assigned to the 9 users with the permission MNR_HLPDSK_PSWD_C. Only Security personnel should be given the authority to reset passwords.

PeopleSoft Financials:

- Management should consider disabling or deleting the user ids for terminated users in PeopleSoft Financials to prevent unauthorized access within the system to maintain consistency in the cleanup efforts as within the PeopleSoft Enterprise Portal.
- Management should consider reviewing all the permissions assigned to the user noted above carried over from the staging environment during the version 9 upgrade. They should determine which permissions he should be given access to as part of his job function. All other permissions should be removed. This will help to protect the integrity of data.

Management should also consider performing a review of the users in PeopleSoft Financials to detect other users who have been assigned excessive privileges during in staging and carried over during the version 9 upgrade. If users are assigned excessive permissions to system resources, then such users will have access to unnecessary system functions and information resources.

Corrective Action Taken

The following corrective actions have been taken on the above findings.

PeopleSoft HR

- 186 user ids in PeopleSoft HR belonging to the terminated users have been deleted from the system.
- The 9 users with the authority to reset passwords have been rectified and their roles have been modified and access removed.

PeopleSoft Financials

- 12 user ids in PeopleSoft Financials belonging to the terminated users have been deleted from the system.
- The PeopleSoft Financials id belonging to the user noted above has been locked and the permissions granted to it have been removed. The user account has since been deleted.

Management's Response:

PeopleSoft HR:

- In order to sign on to our PeopleSoft systems, a user must first sign onto our computer network (LAN), and then must sign on to the PeopleSoft Enterprise Portal. The accounts for the users in question had already been deleted from the LAN, and the PeopleSoft Enterprise Portal, along with any remote access, as part of our standard operating procedures for when an employee separates from the company.

The accounts remained in the HR system because they had not yet been cleaned up by the Security Administrators. However, since the first two required levels of access had already been

removed, the users would not have been able to access the HR system. This would be a mitigating control.

The accounts identified were deleted during the audit.

- This MNR_HLPDSK_PSWD_C component was in a permission list assigned to the Benefits department. This may have been an oversight during the HR implementation. The help desk password reset function is limited to the password reset of the general user population. This function is unable to reset the password belonging to the security group and the external applicant id. This was set by design to prevent security from being locked out of their accounts and to prevent denial of service to external applicants from applying for a position.

PeopleSoft Financials:

- In order to sign on to our PeopleSoft systems, a user must first sign onto our computer network (LAN), and then must sign on to the PeopleSoft Enterprise Portal. The accounts for the users in question had already been deleted from the LAN, and the PeopleSoft Enterprise Portal, along with any remote access, as part of our standard operating procedures for when an employee separates from the company.

The accounts remained in the financial system because they had not yet been cleaned up by the Security Administrators. However, since the first two required levels of access had already been removed, the users would not have been able to access the financial system. This would be a mitigating control.

The accounts identified were deleted during the audit.

- This access was provided in the staging environment during testing of the version 9 financials prior to the upgrade of the live environment. The D&T audit commenced prior to the completion of the system cleanup. All access was removed from this account during the audit and the account was locked to prevent logon.

The account was deleted once it was confirmed that it was not required in a supporting role.

2. CMS Application Security

Observation:

An assessment of the CMS environment identified that the user access request forms for one user could not be obtained. However, a log of the change was recorded in an access table maintained by IT Security.

Background:

To test the process of providing access to new users, we had selected a sample of 5 users. Of these 5 samples selected, the new user access form for one user could not be obtained. This user was provided access to the CMS application on April 5, 2007. However we were unable to obtain the new user access form for this individual.

Recommendation:

User access related documentation should be stored such that information supporting the user's access would be readily available upon request and to determine that only authorized personnel have access to the application.

Management's Response:

The document could not be located; however a log of the change was recorded in an access table maintained by IT Security. Metro-North is considering implementing an electronic version of the access request process by the end of 2008. This will eliminate or drastically reduce the number paper access request forms used. Implementing the electronic access request process will eliminate the misplacement or loss of processed request forms.

SECTION II – OTHER MATTERS

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

1. Missing Birth Date Information from PeopleSoft

Observation:

Certain retirees' demographic information, e.g. birth dates, are not included within the PeopleSoft system.

Background:

Employees who retired in the years 1983, 1984 and 1985 do not have birth dates maintained in the PeopleSoft system. When Metro-North inherited its HR/Payroll data files from Conrail in 1983, the birth date field was not populated. Metro-North completed its own data verification and conversion during 1986, but until that year, birth date data were not reliably available.

When Metro-North established its retiree population on PeopleSoft, data from GEAC were used to populate the retiree data fields. Since birth date data were not available for the years 1983 to 1985, these data are missing in PeopleSoft. When Metro-North sent the data file to Milliman Actuaries, Milliman arbitrarily assigned a birthday of July 1, 1924 to all individuals who retired in 1983, 1984 and 1985. The assumption was that, on average, employees retire at the age of 60.

During testing, D&T was able to obtain the date of birth of an individual who retired between 1983 and 1985 by contacting the Railroad Retirement Board.

Recommendation:

It is recommended that Metro-North contact the Railroad Retirement Board to obtain the birth dates of all employees with a blank date for their respective birth date field in the PeopleSoft system. This will provide more accurate demographic information to the actuary and ultimately allow for a better estimate based upon the actuarial calculation.

Management's Response:

Metro-North concurs with the recommendation. Metro-North will work with the Railroad Retirement Board and expects the missing birth dates to be in the PeopleSoft system by the end of the 4th quarter of 2008.

SECTION III – DEFINITIONS

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

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

A *significant deficiency* is a control deficiency, or combination of control deficiencies, that adversely affects the entity'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 by the entity's internal control over financial reporting.

* * * * *