www.pwc.com

New York City School Construction Authority

December 23, 2014

Report to Management

pwc

December 23, 2014

Members of the Audit Advisory Committee
of the New York City School Construction Authority:

In planning and performing our audit of the financial statements of The New York City School Construction Authority (the "Authority") as of and for the year ended June 30, 2014, 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 was not designed to identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have been identified.

AU 325, *Communicating Internal Control Related Matters Identified in an Audit*, of the AICPA Professional Standards includes the following definitions of a deficiency, a significant deficiency and a material weakness:

> **Deficiency**—a deficiency in internal control 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.
>
> **Significant Deficiency**—a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.
>
> **Material Weakness**—a deficiency, or combination of deficiencies, in internal control 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.

As agreed in our engagement letter, we are providing you with a report of all deficiencies, operational, business and other observations.

If you would like any further information or would like to discuss any of the matters raised, please contact David Mandelbaum, (646) 471-6040.

Very truly yours,

PricewaterhouseCoopers LLP

PricewaterhouseCoopers LLP

PricewaterhouseCoopers LLP, 300 Madison Avenue, New York, NY 10017
T: (646) 471 3000, F: (646) 471 8320, www.pwc.com/us

Table of Contents

I. Significant Deficiency

1. Proper accounting for insurance receivable/liability

Observation:
During the course of the current year audit, we proposed and Management recorded adjustments related to the Authority's accounting for insurance.

The Authority entered into an Owner-Controlled Insurance Program (OCIP) for its General Liability (GL) and Workers' Compensation (WC) coverages with ACE insurance which began January 1, 2014 under a term of one year.

Errors were identified during the review of the detailed schedules related to this policy as provided by the Authority. These errors are related to the timing of recognition in the financial statements. There is no cash impact to the Authority. The errors included:

- Overstatement of the Excess GL liabilities, reducing the amount owed by the Authority by approximately $10m.
- Not identifying the projected reimbursements to the Authority of approximately $38m for 2014 policy year based on the June 30, 2014 valuation in a timely manner.

The adjustments are indicative of a need to improve the Authority's review and analysis of its accounting for insurance.

Implication:
Not appropriately reviewing and analyzing the accounting for insurance policies may result in a misstatement of the Authority's financial statements. The relatively small amount of the potential misstatements compared to total fund balance and net assets, is not deemed a material weakness. However we believe the risk is such that it merited communication to the Audit Advisory Committee and therefore qualifies as a significant deficiency.

Recommendation:
We recommend ensuring the Authority has a formal process to evaluate the financial implications of all provisions of its insurance policies. The primary and excess insurance bought by the Authority is increasingly complex with many moving variables. We recommend full and clear documentation of all policies purchased and in-force, as well as thorough understanding by both Willis and the Authority of their terms to accurately estimate the required accruals.

Management's Response:
Management agrees with this recommendation. The Authority will work together with Willis of NY (SCA Insurance Program Manager) to ensure that the actuary report is comprehensive and incorporates all of the financial implications that are required in the financial statements based on the provisions in the policies. A formal meeting to review the actuarial report will be completed before the report is distributed to the auditors. This review will include the items identified in the finding.

The Authority will discuss this finding with SCA Internal Audit to identify any potential improvements that can be added to the review process.

II. Information Technology Comments

1. Enhance security controls within Expedition Contract Management 13 (CM-13).

Observation

While there was a review of users' access to Expedition, such review was incomplete. Management requested that all business owners review the access rights of their groups. However, there was no review performed on users belonging to the Architecture & Engineer group.

Risk and Impact:
The lack of a timely and effective recertification of users increases the risk of inappropriate access to systems and data. Through time a user's access to the system may no longer be valid due to change in roles or separation from service. Moreover, the periodic review of users can ensure that there is no segregation of duties conflict.

Recommendation:
Management should consider implementing a formal periodic review or recertification of users' access. The recertification process should include the following:

- All active user IDs from the application and their associated access rights
- Analysis of access rights to ensure duties are properly segregated
- All user IDs are uniquely assigned to one individual. If generic IDs are used, individual accountability should be maintained.
- All users IDs belong to a current employee.

Management should ensure that there are set timelines for the reviews, require positive confirmation from each business owner, and retain formal documentation for each review. The documentation should include the evidence of the business owners' response and corrective action taken as a result of the review.

Management's Response:
Management agrees with this recommendation. A process has been designed and implemented to review the more than 2,000 user ids with access to the PCM (CM13). This process entails the creation of security reports for users identifying their access by role and sending the reports to senior staff for review and approval. These reports were sent to contractors and consultants with user access to ensure their employees still required access and that the access level is appropriate. This process was conducted between June and October of 2014 and responses from the different business owners documented. It will be repeated annually for all application users.

2. Enhance monitoring controls of privilege users within CM-13

Observation
There is no logging and monitoring of system administrator activities in Expedition CM-13.

Risk and Impact:
Without the proper logging and reviewing of system administrator activities, there is a risk that access or changes to the systems and/or data are not authorized.

Recommendation:
Management should configure Expedition to capture and log selected system administrator activities based on criticality and risk assessments. These logs should be periodically reviewed to detect any unusual or irregular activities.

Management's Response:
The PCM system has the ability to log all transactions for all users but this program cannot be turned on for specific users such as Administrators only. When this feature is turned on for all users it has a negative impact on the responsiveness and performance of CM-13. Last year we asked Oracle, the owner of CM13, to modify the application so that logging can be turned on for specific users without impact to performance. They informed us that they would not fulfill this request. Accordingly, we have implemented short term modifications to mitigate risk. Our current process requires administrative users to create a service ticket in our helpdesk system known as HEAT once they make any changes in the current production system that affects financial data. The next short term process modification requires a semi-annual review of a sample of transactions that have been created by admin ids in the financial tables and compare them to HEAT tickets for the same date and time period.

Our long term solution is to build a process into the system that will run for admin ids only and capture the transaction records that affect financial data. The system will track the transactions, before and after, when any changes are made and save them in a log table. This will allow IT to develop reports that can identify changes that were made to the production system by the admin ids. This new functionality will be developed by June 30, 2015.

In 2014 the SCA reduced the number of system administrator ids from 15 to 7.