TORONTO TRANSIT COMMISSION
REPORT NO.

MEETING DATE: November 21, 2012

SUBJECT: PRICEWATERHOUSECOOPERS LLP 2011 MANAGEMENT LETTER – FOLLOW-UP REPORT

ACTION ITEM

RECOMMENDATION

It is recommended that the Commission:

(1) Receive for information the attached follow-up report on the PricewaterhouseCoopers LLP ("PWC") management letter; and

(2) Forward the report to the City Audit Committee.

BACKGROUND

At its meeting of October 26, 2012, the TTC Audit Committee received the report for information and approved forwarding the report to a regular meeting of the Commission for information and then to the City Audit Committee.

The PWC audit results report and management letter on internal control recommendations were presented at the April 30, 2012 TTC Audit Committee meeting. A management letter provides recommendations for the improvement of internal controls and accounting processes. Management's initial response to these recommendations was included in the April 30th report. PWC's recommendations and the initial management response are reproduced in the attachment. This is followed by a status update detailing the action staff has taken to address the recommendations.

Based on the City of Toronto Audit Committee July 2004 Report 4, Clause 2 Recommendation 3, the Commission is required to provide an update of outstanding issues raised in the management letter, within six months after the issuance of the management letter.

DISCUSSION

PWC initially provided seven recommendations in the management letter presented at the April 30, 2012 TTC Audit Committee meeting. Of these, one was fully addressed through the initial management response and is therefore not included in this follow-up report. Of the remaining six recommendations, four have since been fully addressed, as detailed in the attachment; and, action is underway to address the remaining two control recommendations. All action taken to date will be subject to review by PWC during the 2012 external financial statement audit.

- - - - - - - - - - - -

November 21, 2012
1-27
Attachment: PWC LLP 2011 Management Letter with October 2012 Update

PricewaterhouseCoopers LLP 2011 Management Letter with October 2012 Update

1.1 Schedules supporting the TTC's capital asset balances, including additions, disposals, depreciation calculation, and capital subsidies should be automated.

Observation

During our testing of capital assets, it was noted that the capital asset process is not automated. Rather, excel spreadsheets are used to track and account for expenditures on capital assets, asset disposals, capital subsidies received and depreciation of capital assets.

Implication

The use of excel spreadsheets to track and account for such significant balances is less secure, more time intensive and increases the risk of error.

Recommendation

Management should investigate capital asset software packages available to automate their capital asset continuity schedules. Doing so will allow the Company to:

- More accurately track capital spending against associated capital subsidies
- Generate a fixed asset continuity schedule, detailing cost and accumulated depreciation, by asset class.
- More easily identify when an asset is put into productive use.
- Reduce the amount of estimation used in determining depreciation expense throughout the year.
- Eliminate the risk that an excel formula or other type of error will go undetected.

In the interim, we recommend that management implement spreadsheet controls around the current excel spreadsheets being used, restricting access through password controls and write-protecting the continuity schedules so that changes cannot be made inadvertently or without appropriate authorization or approval.

April 2012 Management Response

The Capital Asset system in the Worth-It software application has been established for 2006 assets of record and subsequent year capital additions for years 2007-2010 have been entered into the system. Further system testing and realignment of asset groupings continue to ensure that compliance to PSAB requirements and financial statement presentation are correctly being tracked and reported. The tracking of capital expenditures, funding and related capital additions will continue to be handled through spreadsheets under the direct control of Capital Accounting staff to mitigate the risk of changes without proper authorization.

October 2012 Update

Automation of the capital asset update process will be considered as part of the new ERP solution (to be included in the requirements and specifications for the replacement of the financial systems). In the interim, the Worth-It system will be utilized to capture the updated asset information for the Commission's capital assets; however, the use of existing spreadsheet models will still be required to supplement the capture and accumulation of current year capitalization projections and the resultant depreciation. These spreadsheet applications are under the direct control of Capital Accounting staff to ensure that only authorized changes are accepted based on information updates provided by project staff. Staff are continuing to seek improvements in the Worth-It application, supporting spreadsheets and processes which will be incorporated into future updates.

Status

Complete.

1.3 Frequency of cycle counts over less used inventory items

Observation

During our testing of the inventory cycle count process, it was noted that there were numerous inventory items physically counted only once every three years.

Implications

Large inventory 'book to physical' differences might exist for these items due to theft or human error in processing inventory and these differences would not be identified until the inventory items were counted. As a result of these items not being counted more frequently, the inventory balance could be misstated.

Recommendation

We recommend that all inventory items, regardless of how often they are used, should be counted at a minimum once per year.

April 2012 Management Response

The majority of inventory is counted at least once per year (in many cases multiple times per year). Parts that are counted once every three years are slow moving items that are stored at either the Greenwood or Duncan warehouse. These slow moving parts comprise approximately 25% of total inventory value and typically consist of critical spare components or are items that have a low unit value.

Management will review the cycle count processes and consider making some adjustments to the cycle count schedule to count additional stock codes at least once per year where it is warranted. When making adjustments to the cycle count schedule, consideration will be given to additional resources required to undertake the additional counts.

October 2012 Update

The inventory counting process has been changed such that all parts at all locations will be counted at least once per year. As of September 2012, over 88% of the parts have been counted at least once, and the remaining parts will be counted by the end of 2012.

Status

Complete.

1.4 Formalization of the communication protocol between Special Investigations and TTC senior management.

Observation

In the process of completing our audit we noted that there is not a formalized communication protocol between the Special Investigations department and senior management at the TTC to keep them informed of progress on any on-going investigations. It currently is an ad hoc, informal, process.

Implications

Without a formal communication protocol there is the risk that senior management may be unaware of investigations on-going which may impact or involve the departments and/or staff for which they are responsible.

Recommendation

We recommend that formal communication protocols be established whereby the Special Investigations department submits a report, at least quarterly, detailing the investigations that are on-going and the areas impacted.

Management Response

Management will formalize a quarterly report on the progress of ongoing investigations and will report same to the Chief Executive Officer (CEO) and Chief Financial and Administrative Officer (CFAO). The CFAO will forward the information to the City Auditor General. If anything arises that is of critical importance between reports, the CEO, CFAO and Auditor General will be advised accordingly.

October 2012 Update

A formal report of ongoing investigations has been initiated and submitted to the Chief Executive Officer (CEO) and Chief Financial and Administrative Officer (CFAO). These reports will be updated and submitted on a quarterly basis.

Status

Complete.

2.1 Lack of approval on claim payments

Observation

In auditing the claim payment process it was noted that adjusters have the ability to make claim payments within an authority limit while visiting a claimant off-site. Adjusters are permitted to make payments above their authority limit with prior approval from their supervisor.

Implication

There is some risk of an unauthorized payment given that there is no IT system to prevent the release of a bank draft that has been written in excess of an adjuster's limit without the supervisor approval.

Recommendation

The payment process should be automated through the Riskmaster system. Adjusters should need to obtain approval before payment is provided to any claimant.

Automated authority limits for claim payments should also be set-up within Riskmaster. Should a claim payment be outside an adjuster's authority limit the payment should need to be approved and evidence provided to support that the escalated payment is necessary before the payment is provided to the claimant.

Management Response

Currently all adjusters have the authority to write a draft within their individual dollar authority. All adjusters are fully aware that any draft written above their authority without prior approval could lead to disciplinary action up to and including dismissal.

All payments are bank drafts (not cash) and whether the draft is issued in or outside the office, it is processed in the same fashion. All drafts are sequentially numbered when assigned to the adjuster and they are required to verify and sign for the drafts they have been issued.

Once the draft is issued by the adjuster to the claimant and processed through Riskmaster the payment is entered on to a transmittal sheet by Claims department clerical staff. The transmittal sheet lists the draft number and the amount of the draft. The Claims Director reviews the transmittal sheet and the draft copies to ensure that all payments listed are within adjustor's limit. If the amount of the payment exceeds the adjustor's authority, the draft copy would have the supervisor's sign-off, which is verified by the Claims Director. Once this verification has been completed, the payment information is forwarded to Finance. Finance staff reconcile payments processed through the bank, with this record of authorized payments listed in Riskmaster. If Finance staff identify a payment that was not listed in Riskmaster, Claims staff would be immediately contacted to follow-up.

All claimants assigned to an adjuster are done so by Claims Management Staff who have reviewed the reports and confirm the incident. The adjusters have no prior knowledge as to which claimant they are going to be assigned.

In addition to the controls already in place, staff are in contact with Riskmaster personnel and are in the process of investigating the required process and system modifications that would be required to implement the recommendation wherever possible given both system limitations and operational requirements.

October 2012 Update

To implement this recommendation, cheques need to be produced through the Riskmaster system. The current version of Riskmaster does not produce cheques that conform to Canadian cheque clearing requirements. This issue needs to be resolved before the recommendation can be implemented. A review is currently ongoing on an updated version of Riskmaster to ensure that the Canadian cheque clearing requirements can be met, with the goal of implementing a new version of Riskmaster and the PWC recommendations in 2013.

Status

In Progress

3.1 User access considerations

Observation

During our audit procedures, we noted a number of user accounts within Payroll, MMS/IFS, Risk Master and Millennium with respect to terminated employees were not removed on a timely basis. We also noted that the TTC security policy does not establish a time frame in which user accounts are cancelled after the termination of an employee.

As well, we noted that user access reviews for super users are not performed to ensure user access is appropriate at the database level (e.g. Windows, SQL and Oracle).

Implications

Unauthorized transactions could be performed or unauthorized access could be obtained.

Recommendation

User access for terminated employees should be removed within 5 days of employment termination. The TTC Information Security policy should require that staff terminations be communicated to the IT department in a timely manner to ensure that terminated employees no longer have access to the system.

A super-user access review should be performed at least once per year or according to TTC risk considerations. This review should be performed by an individual without administrative privileges. Any exceptions noted should be properly disabled.

Management Response

User access to the primary environment (i.e. the Windows Server Domain) is removed immediately upon the receipt of an employee termination notification.

However, Information Technology Services Department will streamline the user access termination process for secondary environments (i.e. mainframe, applications, databases, CICS and CMS) by having the Access Control Administration Section coordinate the termination of user access across the departments in a timely manner. This process will be initiated upon the receipt of an employee termination notification from Human Resources Department or from an employee's immediate supervisor to ensure that access to the primary and secondary environments of each terminated employee is removed.

The following changes will be made to improve the access termination process:

1. Improvements to termination notification process will be undertaken and targets for complete access removal will be established; and
2. Once the process is established, the corporate security policy will be updated to reflect the changes.

We agree. A listing of super and/or privileged user accounts at database and operating system level will be produced once a year and will be reviewed for exceptions by the Information Security Office.

October 2012 Update

A procedure for disabling access for terminated employees has been drafted and includes a requirement to remove IT access within 5 days of termination. A super-user access review will also be performed each year by the Information Security Office. This review will be completed by the end of 2012. For critical users the removal process is immediate based on notification of IT management.

Status

In progress.

3.2 Password security parameters could be strengthened

Observation

During our audit, we reviewed the password settings on the Voltage and Pistons servers and noted that the password aging settings were “disabled’ and there were no security guidelines in the TTC’s security policies about super-user password management.

As well, we reviewed the password settings within the mainframe and noted that the password length for all users is set at four characters. We also noted that Great Plains and Risk Master do not have the typical security features on passwords such as requiring passwords to be minimum of six characters in length, requiring the use of an alpha-numeric passwords, not allowing the same password to be used twice etc.

Implication

Account passwords should be changed with scheduled frequency to reduce the risk of unauthorized access or transactions.

Weak password controls also increase the risk of unauthorized access or transactions.

Recommendation

We recommend that users should be required to change their passwords at least every 90 days. Password lengths should be set at a minimum of at least six characters and alpha-numeric passwords should be required.

Management Response

Server Technology, after review with PWC, confirmed that password aging was disabled and that Server Technology will enable the password aging in the UNIX environment.

The Corporate Security Policy will be reviewed and updated to reflect the changes recommended by PwC regarding the password management of super user or privileged accounts, including service accounts as deemed appropriate.

Server Technology will adjust system settings on the mainframe environment such that the minimum password length will be six characters. The current maximum number of lockout attempts will remain at three. The Corporate Security Policy will be reviewed and updated to reflect the changes recommended by PwC about Password settings and lockout account attempts as deemed appropriate.

RiskMaster and Great Plans administrators will implement, where possible, the following steps to better enforce the setting of password parameters:

1. Enforce Password Policy: Users to adhere to the same password policies that have been established on the Windows Server domain;
2. Change Password Next Login: Users to change their passwords the next time they log into Microsoft Dynamics RM;
3. Enforce Password Expiration: Users to change their passwords after the number of days that is defined by the Windows Server domain password policies; and
4. Enforce Password Complexity: Users to make the choice of selecting a password a little more difficult rather than, for example, 12345. Users will make sure that they have capital letters, small letters, special characters, numbers, etc. when selecting passwords.

In addition to the above, RiskMaster and Great Plans administrators will review access rights periodically in order to eliminate the risk of unauthorized access.

October 2012 Update

Password aging is now enabled in the Unix environment and users will be required to change their passwords every 90 days. Password settings for the Mainframe environment as well as for RiskMaster and Great Plains have been adjusted to require a minimum of 6 characters, with standard password complexity requirements. An annual review of Riskmaster and Great Plains users is also prepared and reviewed.

Status

Complete