Form Revised: February 2005

TTC AUDIT COMMITTEE REPORT NO.

MEETING DATE: April 30, 2012

SUBJECT: INTERNAL AUDIT – INFORMATION TECHNOLOGY SERVICES DEPARTMENT - CLIENT SERVICES

INFORMATION ITEM

RECOMMENDATION

It is recommended that the Audit Committee receive for information the attached Internal Audit Report.

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

Joseph L. Kennelly
Chief Auditor (Acting)

April 30, 2012
01-27

Attachment – Internal Audit Report

TORONTO TRANSIT COMMISSION
INTERNAL AUDIT

EXECUTIVE BRANCH

INFORMATION TECHNOLOGY SERVICES DEPARTMENT

CLIENT SERVICES

Covering Period:
January 2010 to June 2011

FINAL AUDIT REPORT – File No.: 10-50032 **OCTOBER 2011**

TABLE OF CONTENTS

Page No.

EXECUTIVE SUMMARY

This audit assessed the key management and operational controls of the Client Services area in the Information Technology Services (ITS) Department. An Exit meeting was held on November 4, 2011 with the General Manager, Executive Branch, Chief Information Officer and the Director – Client Services to discuss the audit findings.

Client Services operates with an approved 2011 budget of approximately $2.1 million and a staffing level of twenty-five positions.

Audit found that the areas are generally well managed and controls are in place. However, Audit identified several areas which required strengthening of the existing controls to minimize risk exposures and costs.

Audit recommended the strengthening of the contract administration controls to ensure technical service assistance is acquired in accordance with TTC requirements. Policies relating to computer security should be reviewed and updated, as required, to ensure TTC information and assets are protected. Management agrees with the recommendations and corrective action has been implemented to strengthen controls.

We wish to express our thanks for the cooperation and assistance from all staff during the course of the Audit.

J.L. Kennelly
(Acting) Chief Auditor

FOREWORD

Client Services is one of six sections within the ITS Department. The section has responsibility for the management of the service desk (which includes incident and problem management), developing and maintaining a service level management process, establishing an information security policy and maintaining an information security network across the TTC.

Other responsibilities include contract administration, document management and administrative support for the ITS Department.

AUDIT SCOPE AND OBJECTIVES

Scope

A review of key management and operational controls within the Client Services section for the period January 2010 to June 2011.

Objectives

To assess the management and operational controls to ensure:

- accountability and reporting relationships are appropriate for the Commission
- due regard for economy, efficiency and effectiveness
- procedures and processes are in place to measure and report on key activities

To evaluate the adequacy of financial controls to ensure:

- compliance with legislative and TTC requirements
- the timeliness, accuracy, completeness and authorization of transactions and data
- the safeguarding and control of assets, and other sensitive information

AUDITED ITEMS FOUND ACCEPTABLE

KEY CONTROL	FINDING
Security Desk/Access Control Administration	Information technology (IT) inquiries and problems, including computer access requests, are resolved and tracked effectively.
Documentation Management	ITS documentation is managed in accordance with departmental documentation control and review procedures.
Hazard Identification and Risk Assessment (HIRA)	A HIRA has been prepared and approved for each section within the ITS Department.
Operational Control Reporting	Relevant reports are produced to assist management decision-making and measuring progress against stated targets.

FINDING #1

CONTRACT ADMINISTRATION

OBJECTIVE: To determine that technical service assistance is economically acquired through the Global Technical Assistance (GTA) contract in accordance with TTC policies and requirements.

ANALYSIS: The ITS Department supplements permanent IT staff with technical expertise from external placement firms through the GTA contract to meet system project requirements which are part of the approved Capital Program. In 2006, the Commission authorized the TTC to award a GTA contract with a total upset limit (including amendments) of $55.1 million to eight companies expiring on August 31, 2011.

Audit reviewed a sample of twenty-five contractor files out of a total population of 111 contractors. The following process controls and business practices were noted where improvement is required:

Contract Requisition and Approval
In the sample of twenty-five contractors, Audit noted an instance where a candidate was selected based on their soft skills and not on the candidate's interview score; and, another instance was noted where the second place candidate was acquired rather than the one with the higher score.

Interviews are also held in secured buildings which could pose a security risk, i.e., the Patten Building (Revenue Operations) at Hillcrest.

Contract Extensions
Justifications for two contract extensions were found not in accordance with the contract requirements. Audit noted the following:

- One contract was extended for a new work assignment which reassigned the contractor from an Analyst position to the Project Lead rather than referring the new work request to the GTA vendors.

- The GTA process limits contract extensions to two. However, one contract was extended four times. Although special approval was received for the third extension, Audit found no evidence to indicate special approval was obtained for the fourth extension.

Overtime

Monitoring of overtime incurred by contractors is not effective to identify unusual amounts of overtime earned. In Audit's sample testing, five of the contractors reviewed cumulatively worked 1,227 hours from January 2010 to June 2011, for a total of $93,278 in overtime pay. Weaknesses identified in the monitoring of overtime include:

- Overtime hours worked were found lacking evidence of pre-approval. In a sample of fifty invoices, eighteen of the invoices included billings for overtime hours and evidence of approval was only observed on four of the invoices.

- Overtime requests are sent for approval after the hours are worked.

- A 'blanket' overtime pre-approval was issued to enable contractors to work up to ten hours of overtime per week for four months.

Contract Deliverables and Performance Evaluation

Audit noted that two of the twenty-five contracts reviewed were lacking clearly stated deliverables, e.g., Quality Assurance Analysts were acquired for contract work described as on 'various' projects. The lack of clear deliverables can lead to open-ended work assignments.

The method used to evaluate contractor performance has been identified by TTC's Human Resource Department as inappropriate and has recommended changes be made to ensure a clear distinction exists between the roles for contractors and employees.

RECOMMENDATION: Management should ensure:

- a standard interview evaluation method is used for all candidate interviews, and interviews are held in TTC office areas which do not pose a significant security risk exposure
- contract extensions for new work are supported by documented justifications and appropriate approval authority
- overtime is approved and controlled in accordance with TTC requirements
- contracts have clearly stated deliverables and performance evaluation of contractors is in accordance with Human Resources requirements

MANAGEMENT RESPONSE:

Contract Requisition and Approval

- In the sample of twenty-five contractors, Audit noted an instance where a candidate was selected based on their soft skills and not on the candidate's interview score; and, another instance was noted where the second place candidate was acquired rather than the one with the higher score.

  Response
  IT Management concur that this finding is true for one candidate.

  After reviewing evidence provided it should be noted that the candidate with the highest rating, after the interview process was held in March, would not be able to commence his employment with the Project until sometime in June. A decision was made by the Supervisor that this would cause too much of a delay to the project and therefore the second highest candidate was selected.

  In future, IT Management will ensure that deviations to the hiring process are more clearly documented.

- Interviews are also held in secured buildings which could pose a security risk, i.e., the Patten Building (Revenue Operations) at Hillcrest.

<u>Response</u>
The interview in question was conducted by members of another Department who were being allowed to hire a contractor under the auspices of the IT Services GTA Contract. The interviewers conducted the interviews on site at their location, which in this case was the Revenue Operations Building, a secure site. Management has noted Internal Audits finding and will ensure that, in future, no interviews will take place in any area that could pose a security threat to the TTC.

<u>Contract Extensions</u>

- One contract was extended for a new work assignment which reassigned the contractor from an Analyst position to the Project Lead rather than referring the new work request to the GTA vendors.

  <u>Response</u>
  IT Management reviewed the evidence provided regarding this finding. A memo written by the Project Manager to her Director requesting a second extension, permissible under the GTA contract, contains the following wording, "Now that this project has resumed, I would like to assign XXXXXX to the lead role." There is no evidence in the extension documentation that any deliverables had changed, nor was there a change in the title of the position. IT Management are of the belief that the Project Manager was following the published process for extending Contractors and was not asking for any change in deliverables or job title in doing so. Should there have been any evidence of a deliverable change the Project Manager would have had to submit a new requisition for posting amongst our qualified vendors. In future, the Contract Administrator will further review all documentation submitted for file to ensure that they are clear, leaving no room for interpretation.

- The GTA process limits contract extensions to two. However, one contract was extended four times. Although special approval was received for the third extension, Audit found no evidence to indicate special approval was obtained for the fourth extension.

  <u>Response</u>
  There was a single individual who was extended four times. The initial placement was for a period of one year. The first extension was intended for a period of 24 months, however, the agency agreement only had twenty

months left at the time. Once the new agency agreements were in place this individual was "extended" for the remaining 4 months of the initial extension. A second extension in accordance with the approval process was granted. Due to project complexity, a third was provided as the specific knowledge of the contractor was required. The final extension was to retain the specialist until project completion. All future contract extensions will follow the documented approval process. Any exceptions to this will require the approval of the Manager – Materials and Procurement and the General Manager – Executive.

<u>Overtime</u>

- Overtime hours worked were found lacking evidence of pre-approval. In a sample of fifty invoices, eighteen of the invoices included billings for overtime hours and evidence of approval was only observed on four of the invoices.

  <u>Response</u>
  From time to time, contractors are required to work overtime when they are not able to contract their Supervisor. Those hours are approved asap following the work. If not approved by the Supervisor, the hours would not be paid.

- Overtime requests are sent for approval after the hours are worked.

  <u>Response</u>
  IT Management concur, however, at times during projects it is necessary for contractors to work overtime where they do not have the ability to contact their Supervisor for preapproval. IT Management would like to note however, that there are controls in place that allow Supervisors to reject payment for overtime worked without preapproval. As noted above, Contractors are responsible to enter their work hours into the Time Control system that Supervisors are required to review and approve. Should the Supervisor note that there were hours of work documented that the Supervisor did not approve at anytime, i.e. Before or after completion of the work, the Time Control entry would not be approved and the hours worked would not be paid.

- A 'blanket' overtime pre-approval was issued to enable contractors to work up to ten hours of overtime per week for four months.

Response
IT Management concur and will ensure that the process clearly defines that this method of managing overtime approvals is not permitted. IT Management will further ensure that the only method of allowing for overtime is for preapprovals on a one time basis only.

Contract Deliverables and Performance Evaluation

- Audit noted that two of the twenty-five contracts reviewed were lacking clearly stated deliverables, e.g., Quality Assurance Analysts were acquired for contract work described as on 'various' projects. The lack of clear deliverables can lead to open-ended work assignments.

  Response
  IT Management concur and have revised the wording in the requisition template to read, "Other projects may be assigned on an ad hoc basis to assure full utilization of contractor resources."

- The method used to evaluate contractor performance has been identified by TTC's Human Resource Department as inappropriate and has recommended changes be made to ensure a clear distinction exists between the roles for contractors and employees.

  Response
  IT Management concurs and will be updating the contractor performance process. IT Management will also be requesting a review of this update by the Human Resources Department.

Completion Date: **Quarter 3 – 2012**

Responsibility: **Director – Client Services**

FINDING #2

INFORMATION SECURITY OFFICE (ISO)

OBJECTIVE: To determine that an integrated information protection program is in place and maintained to protect TTC information.

ANALYSIS: The ISO is responsible for ensuring that information security requirements are applied and integrated to ensure information systems are protected from threats to confidentiality, integrity and availability. This involves setting and promoting awareness of computer security policies and standards for use throughout the TTC.

Audit's review and discussions identified the following areas where further improvements can be made to protect the TTC's information resources:

a) ....
ccountability and responsibility roles for computer security over TTC's industrial computing assets have not been established and defined in the TTC Corporate Policy 7.2.2 Computer Security – Assets and Information. Unclear responsibility over information security for industrial computing systems could result in the lack of security protection for industrial computing information and systems failure.

b) ....
omputer system contracts entered into by other TTC Departments are not provided to the ISO for review to ensure compliance with TTC's computer security requirements. The lack of ISO review can increase the risk that the TTC could enter into computer system contracts which expose the TTC to IT security vulnerabilities.

c) ....
he User Awareness program has not been updated to ensure TTC employees are informed and aware of IT security risks and TTC's computer security policy.

d) ....
TC does not have an Intrusion Detection and/or Prevention System to protect and prevent critical TTC

computer systems from malicious activity.

RECOMMENDATION: Management should:

- pdate the Computer Security Policy to define the accountability and responsibility roles for computer security over TTC's industrial computing assets

- nsure that IT system contracts are reviewed for compliance with TTC's computer security requirements

- pdate the User Awareness program to ensure TTC employees are informed of IT security risks and TTC's computer security policy requirements

- onsider implementing an Intrusion Detection and/or Prevention System to protect and prevent critical TTC computer systems from malicious activity

MANAGEMENT RESPONSE:

<u>Finding a)</u>

Accountability and responsibility roles for computer security over TTC's industrial computing assets have not been established and defined in the TTC Corporate Policy 7.2.2 Computer Security – Assets and Information. Unclear responsibility over information security for industrial computing systems could result in the lack of security protection for industrial computing information and systems failure.

Response

Responsibilities for computing systems will be reviewed and updated, as required, in Corporate Policies. Further, IT Management recognize that as part of these policies the Operations Branch has clear responsibility over industrial computing assets. However, IT Staff currently meet on a regular basis with Operations Branch staff to aid them in ensuring that they are working towards compliance, where possible, to TTC Policies. IT Management will continue to

ensure that staff maintains these meetings and continue to offer any assistance to Operations Branch Staff when needed.

Completion Date: **Quarter 3 – 2012**

Responsibility: **Director – Client Services**

Finding b)

Computer system contracts entered into by other TTC Departments are not provided to the ISO for review to ensure compliance with TTC's computer security requirements. The lack of ISO review can increase the risk that the TTC could enter into computer system contracts which expose the TTC to IT security vulnerabilities.

Response

IT Staff will review with all Departments to ensure that purchases including computer systems address appropriate compliance with security risk.

Completion Date: **Quarter 3 – 2012**

Responsibility: **Director – Client Services**

Finding c)

The User Awareness program has not been updated to ensure TTC employees are informed and aware of IT security risks and TTC's computer security policy.

Response

Ongoing awareness is performed through e-mail, New Employee Orientation courses at Human Resources (as well as New IT Employee Orientation in the IT Department), updates at IT Rep meetings, signing of Employee Conduct documentation to demonstrate knowledge of Corporate Policies including those involving IT security as well as a dynamic intranet site. The Information Security Office is also responsible for reviewing any changes in security issues which might warrant a further update to security awareness.

Completion Date: **Quarter 3 – 2012**

Responsibility: **Director – Client Services**

Finding d)

TTC does not have an Intrusion Detection and/or Prevention System to protect and prevent critical TTC computer systems from malicious activity.

Response

IT Management concur that an Intrusion Detection/ Prevention system is not in place. However, it should be noted that other numerous security initiatives are in place in order to protect TTC assets. These include, but are not limited to, policies, procedures, internet monitoring, security appliances and/or software as well as External Intrusion Audits. IT Management will continue to review the need for further security enhancements, including the possibility of implementing intrusion detection/preventions systems, and will address any future needs as part of the budget approval process.

Completion Date:	**2013 budget cycle**
Responsibility:	**Director – Client Services**