April 27, 2007

Councilor Chad Collins  
Chair of the Audit & Administration Committee  
City of Hamilton  
71 Main Street West, 1st Floor  
Hamilton, Ontario  
L8P 4Y5

Dear Councilor Collins:

At the completion of the 2006 audit of the City’s financial statements each year we, as the external auditors, prepare a letter outlining areas where control structures and internal controls could be strengthened.

Enclosed is the letter arising out of the audit of the 2006 financial statements. We have included management’s response in this letter.

We look forward to addressing the committee on the issues discussed in this letter.

Yours truly,

GRANT THORNTON LLP

Evan McDade, CA, CBV  
Partner

cc. Glen Peace, City Manager  
Joe Rinaldo, General Manager
April 27, 2007

Audit and Administration Committee
City of Hamilton
71 Main Street West
Hamilton, Ontario
L8P 4Y5

Dear Committee Members:

RE: Internal Control Findings from the 2006 Audit

We have audited the financial statements of the City of Hamilton as at December 31, 2006 for the year then ended, and reported thereon to the members under the date of April 27, 2007.

Our approach to internal control involves gaining an understanding of the Corporation’s controls pertinent to reliable financial reporting and evaluating our findings against the internal control framework. More specifically, our process this year involved:

- understanding the processes that impact financial reporting
- documenting an understanding of the controls within the tax revenue, water and sewer revenue, grant revenue, employee compensation and operating expense cycles that prevent or detect errors, including fraud
- assessing the effectiveness of the design of those controls and identifying potential controls “gaps”, operating deficiencies, and other weaknesses or advisory comments

The standards of the public accounting profession require us to report annually to you our findings on weaknesses and deficiencies in your internal controls. The accounting standards require that the internal controls letter/management letter contain all material weaknesses and significant deficiencies regardless of their practicality or management’s current ability to correct the weaknesses or deficiencies.
Information Technology

We are pleased that several other IT recommendations made in prior years were implemented in 2006. The following information technology (IT) items were identified in prior years and have not yet been fully resolved.

1. Segregation of Duties: Security Responsibilities

As noted in the 2005 internal control letter, our review of the controls related to PeopleSoft (HR & Financial) access privileges revealed that Peoplesoft (PS) developers are assigned with the security responsibility to setup and update user accounts in the PS HR production environment.

Implication
There are privacy concerns where confidential personnel information may be inadvertently revealed or obtained. In addition, unauthorized activities may be entered into the system undetected.

Recommendation
We recommend that IT staff revoke the developers’ view access and ability to setup and update user accounts in the PS HR production environment.

Management Response
IT is required to perform the PeopleSoft HR security updates due to the technical complexity involved. The ability to perform security updates on the HR system is currently limited to only three (3) IT PeopleSoft developers and there exists a low risk of unauthorized activity in this area.

2. Sharing of Generic Accounts

Our review of the network and database user accounts revealed that the System provided “administrator” account is shared by the network administrators (10 individuals). They all have a unique account of their own.

Implication
When user accounts are shared by multiple employees, a lack of accountability exists.

Recommendation
The City should look at implementing policies and procedures to restrict the practice of user account sharing and enforce the practice of assigning each user with a unique user account.

Management Response
The use of the network administrator account by Network Support staff will be changed and in 2007 will result in the ability to track activities performed by each individual account.
3. **IT Change Management Process**

Our review of the application change management process revealed the following:

a. There is no evidence (test plan, test cases, test scenarios, and test results) in place to support that adequate testing was in fact performed.

b. IT management does not review and signoff on changes that are requested for production releases to ensure that only authorized changes are requested and ultimately released.

c. No set guidelines to stipulate the rigor and extent of the testing that is needed for significant or non-significant projects.

**Implication**

Untested, unauthorized, or erroneous codes may be introduced into production and compromise data and system processing integrity.

**Recommendation**

We recommend the following:

a. Maintain testing related documents as audit trail.

b. Conduct IT management review of all changes requested for production releases.

c. Develop testing guidelines that defines when testing is required, the extent of testing (i.e. unit testing, system testing, dependence testing, integration testing, and volume testing, etc), the test plan, and review of the testing.

d. Incorporate the aforementioned review and testing procedures into the IT change management policies and procedures.

**Management Response**

A Change Approval Board (CAB) was established to approve and authorize significant changes to the IT environment. Testing guidelines will be established in 2007.

4. **Password Policies**

Our review of the password settings at the operating system, network, database, and application level revealed the following areas for improvement:

**System Enforced Password Change**

CLASS: no forced password change

Avantis: no forced password change

Vailtech: no forced password change

Hansen: no forced password change

**Password Complexity (requires a combination of alphabets, numbers, upper case, and symbols)**

CLASS: no complexity rules

Network: no complexity rules

PS: no complexity rules

Avantis: no complexity rules

Vailtech: no complexity rules

Hansen: no complexity rules
Account Lockout after a Number of Unsuccessful Attempts
Network: locks account after 3 logon failures. However, the account is unlocked automatically after 15 minutes
CLASS: no account lockout rule
Avantis: no account lockout rule
Vailtech: no account lockout rule
Hansen: no account lockout rule

Account Logoff after a period of Inactivity
Accounts at the network and application level do not automatically logoff after a period of inactivity.

Implication
Weak password policies increase the risk that users may guess passwords and gain unauthorized access to the system and its data.

Recommendation
According to industry best practice, the City should:
• Configure the systems to enforce password changes regularly (i.e. 30 to 60 days)
• Enforce password complexity by require a combination of 3 out of the 4 complexity elements (i.e. require a combination of alphabets, numbers, upper case, and symbols)
• Lockout accounts after 5 unsuccessful logon attempts. Implement the ideal setting of “Forever”. This setting will force users to call the System Administrator to reset their user accounts as opposed to waiting for a specific time period until when the lockout counter is reset.

Management Response
Network password changes are currently enforced regularly on a 90 day cycle.

Network password complexity rules were enforced at the network level in 2006. The password complexity feature is not available in the other above stated applications, and therefore, cannot be implemented.

Network account lockouts are currently set to occur after 3 unsuccessful logon attempts. These lockouts expire after 15 minutes. Many City network users work beyond the scheduled work day hours, 8:00 am -5:00 pm, of the Help Desk. A permanent lockout would prevent many staff from being able to accomplish their work outside the Help Desk hours. The implementation of a permanent account lockout would require additional staff resources to be assigned to the Help Desk to deal with the increased call volumes and the after-hour support. The account lockout feature is not available in the other above stated applications, and therefore, cannot be implemented.

5. IT Policies & Procedures

The City of Hamilton is in the process of developing an overall IT Security policy. The sub-policies of this overall policy included (but are not limited to):
• Information Protection
• Perimeter Security
• Virus Protection and Prevention
However, our review revealed that the City of Hamilton has not considered establishing, documenting, and communicating policies and procedures related to:

- Acquisition and maintenance of hardware, software (OS & Applications), and infrastructure
- Change control management - hardware, software, and infrastructure
- IT facility physical security policy
- Data security (i.e. classification of data, encryption, identify data owner, data back and storage, etc)
- Help desk policy
- New user set-up policy
- Access privileges for terminated employees

**Implication**

When IT policies and procedures are not established, documented, communicated, and distributed to provide a minimum baseline for IT operations, it may lead to operational inefficiencies, weakness in controls, and IT activities not properly understood and executed or evidenced with audit trails. For example, a lack of a testing policy may result in inadequate testing which could increase the risk of insecure or unstable software being improperly installed into the production environment.

**Recommendation**

The City should develop the aforementioned policies and procedures to compliment the overall IT security policy.

The effort and IT controls/procedures introduced through these documents need to be cognizant of the size and complexity of The City of Hamilton’s current operations.

**Management Response**

IT staff currently follow the City’s purchasing policies for acquisition and maintenance of hardware, software (OS & Applications), and infrastructure. The City’s IT Strategic Team will be developing policies in the next 12-24 months.

6. **Disaster Recovery Plan (DRP)**

The City of Hamilton has not finalized its IT DRP. Section 7.0 of the draft DRP was last revised in April 2003.

**Implication**

A DRP provides consistent procedures for employees to follow to enable timely restoration of mission critical systems in the event of a disaster. Unplanned recovery efforts may lead to prolonged system outage and revenue loss.

**Recommendation**

- Finalize the DRP as soon as possible.
- Distribute and test the plan on a regular basis (annually at a minimum) to assess whether recovery requirements support the current technology and employees are well versed in the procedures.
- Management reviews the plan on a regular basis to determine whether significant business, environment and technology changes are reflected in the plan.

**Management Response**

*An external consultant was contracted to perform a business impact analysis and risk assessment. The results will be used to update the DRP. However, the DRP has yet to be tested.*

It is management and the committee’s responsibility to weigh the costs of implementing controls against the benefits that the controls will achieve. The purpose of this letter is to provide you with the information related to the identified risks so that you can make the necessary decisions.

The matters discussed herein are those that have been noted as of April 27, 2007, and we have not updated our procedures regarding these matters to the current date. In addition, this communication is prepared solely for the information of management and is not intended for any other purposes; we accept no responsibility to a third party who uses this communication.

Thank you for the opportunity to contribute to the present and future success of the City of Hamilton.

Yours truly,

**GRANT THORNTON LLP**

Evan McDade, CA, CBV
Partner