ASSURANCE AND ADVISORY
BUSINESS SERVICES

November 24, 2005

Ernst & Young

Quality In Everything We Do

City of Ottawa

Management Letter

Year ended December 31, 2004

ERNST & YOUNG

Ernst & Young LLP
Chartered Accountants
100 Queen Street
Suite 1600
Ottawa, Ontario K1P 1K1

Telephone: (613) 232-1511
Fax: (613) 232-5324

November 24, 2005

PRIVATE AND CONFIDENTIAL
Mr. Lloyd Russell
Director of Financial Services
City of Ottawa
110 Laurier Avenue West
Ottawa ON K1P 1J1
Dear Mr. Russell:

Re: Fiscal 2004 Management Letter

As part of our audit of the financial statements of The City of Ottawa for the fiscal year ending December 31, 2004, we evaluated the company's system of internal controls to the extent we considered necessary under Canadian generally accepted auditing standards. This is done to establish a basis for reliance on systems and determining the nature, timing and extent of other auditing procedures necessary to express an opinion on the company's financial statements. This study was not designed to determine whether the The City of Ottawa's system of internal controls is adequate for management's purposes.

Our audit of the financial statements will not necessarily disclose all conditions requiring attention in the system of internal control because both the audit and study employed, as is customary, selected tests of accounting records and related data. However, our audit identified areas where internal controls could be strengthened and the attached memo is enclosed for your information and further consideration.

All suggestions and comments outlined in the memorandum concerns systems only and are not intended to reflect in any way upon your personnel.

We would be pleased to discuss this document or to respond to any questions at your convenience.

Sincerely,

Ernst & Young LLP

André Bussière
Deanna Monaghan

Enclosures
cc. Mr. Wayne Martin, Manager, Accounting and Financial Reporting, City of Ottawa

Contents

OC Transpo — Inventory Records — St. Laurent Warehouse

Observation and Recommendation

As reported in prior years, some OC Transpo St. Laurent warehouse items (e.g., bus seats and gas tanks) are not in the computerized inventory control system. All items in the warehouse should be included in the SAP inventory listing similar to other rebuilt inventory items.

Management's Comment

These items were excluded from inventory control because of their physical characteristics and low to non-existent residual disposal values. Fleet requirements for seats of this type are quickly becoming obsolete with another 30% of the Fleet using these seats planned to be declared surplus in 2006. Fuel tanks will be brought into inventory for 2006 as the new buses are increasingly using a more valuable Stainless construction. The current value though remains at $ 47,000.

Timing of Inventory Counts

Observation and Recommendation

The majority of high volume inventory items are counted very early in the year. This increases the risk that significant discrepancies between stock on hand and the inventory system amounts at the end of the year will not be identified. High volume items in inventory should be counted in the later half of the fiscal year.

Management's Comment

In 2005 we have made improvements to our counting process during the year which answers this concern. This resulted in a 100% item count representing 100% of the inventory value and a 2nd count that included all new items added during the year. The second count captured 78% of the inventory value. For Year 2004 the cycle count process occupied staff during the entire year. This process is applicable to future counts.

Inventory Not Counted

Observation and Recommendation

We noticed that newly stocked items were not subject to cycle counts during the year because the inventory listing used to perform the counts is the listing at the beginning of the fiscal year. New inventory items should be identified to ensure that they are included in the inventory cyclical counts.

Management's Comment

As discussed above in 2005 process changes allowed us to count the additional 176 inventoried new stock items.

Water and Sewer

Observation and Recommendation

As indicated in the prior year, there is no review of the "DOC Report" in AquaCIS at the management level. The "DOC Report" lists all adjustments based on consumption (i.e. changes to meter reads). There is also an "Adjustment/ Service Charge Report" which lists all adjustments based on transactional basis (i.e. reversal of interest). Both of these reports are generated the day after the adjustments are made and show the operator who made the adjustment. In essence, these reports list all non-routine entries. Review of these reports is important given that anyone with access to AcquaCIS is authorized to make adjustments.

Management's Comment

All material adjustments recorded by the operator are pre-approved by the managers. The Supervisor/coordinator performs a full review daily of both the "DOC Report" and the "Adjustment/Service Charge Report". Management will take additional steps to complete a cursory review and initial both reports after the Supervisor/Coordinator has completed an in depth review.

Provision for Doubtful Accounts

Observation and Recommendation

The City provides for "Trade" Accounts Receivable (A/C 100501) at a rate of 25% for accounts uncollected after 90 days. However, we noted that an amount of $2,774,447 was uncollected after 365 days as at the end of 2004. Since there is a very high risk that such past due accounts will not be collected, the rate used for the provision should be significantly higher than 25%.

Management's Comment

Staff review of actual write-off's show a write-off rate of 0.49% for accounts aged 91 to 120 days and 20.55% for accounts aged 121 days or greater for 2003. For 2004, review of actual write-off's show a write-off rate of 1.69% for accounts aged 91 to 120 days and 14.84% for accounts aged 121 days or greater. Staff will continue to monitor actual write-off's closely and review the estimated rates against actuals. It is important to note that $1.55 million of the $2.77 million are accounts under review by the originating department, assigned to legal for litigation and some have since been paid.

Network Logical Access Review Process

Observation and Recommendation

We noted during our review that Network accounts and profiles have never been reviewed as required by the City "Network Account Management Policy".

The Organization is exposed to the risk that the logical access privileges granted may not be appropriate or that terminated employees will retain previously granted logical access privileges to the system.

We recommend that the Organization perform a clean-up of user accounts and their access to ensure that accounts properly belong to active employees, privileges are appropriate and segregation of duties is enforced. This will provide a clean baseline starting point for the procedures in place.

We also recommend that formal procedures be established for the routine review of logical access privileges on a periodic basis by user management to determine if all users have appropriate access to critical corporate information and data. This procedure allows management to monitor user access, detect any unauthorized or suspect activity and reduce the inherent risk in the distribution of sensitive corporate information assets.

Management's Comment

The IT Services and Employee Services branches of the Corporate Services department have integrated the process for employee staffing actions (e.g. hiring, employee departures) and the process for controlling network access and profiles (e.g. network and e-mail accounts created/deleted) into a single workflow through an enterprise directory system (EDS).

Building on the benefits of having an enterprise-wide SAP HR database, the new automated process improves electronic information security by ensuring that employees have the proper access privileges, based on their job function, and that accounts are deleted promptly when employees leave the organization.

The new process identifies the network and e-mail account requirements for each position and records this information within the SAP HR database. Then, as employees move in and out of positions, the network and email account requirements are automatically communicated to IT Services by the Employee Services Branch. All network accounts for term employee and contractors have a termination date. The enterprise directory system also provides automated e-mail notifications to Managers of pending account termination, ensuring that accounts get disabled on a timely basis.

As part of the implementation of this improved process, the project team performed a wholesale review of all user accounts to ensure a complete synchronization with the SAP HR database.

Internet Access

Observation and Recommendation

We noted during our review that it is possible to access the internet by simply plugging an Ethernet-enabled computer into a commonly available data port, without being a known and authorized member of the City domain.

There is a risk that an unauthorized individual can sniff data packets circulating on the network and decode them by gaining access via one of these data ports.

While we recognize that this internet access granting is mostly a commodity provided by the City to its numerous visitors, but we strongly recommend that the City, at a minimum, closely monitor the network activities and considers segregating the internet access points dedicated to visitors on the City network.

Management's Comment

In mid 2005, the ITS Branch initiated a Network Security Assessment review using external security experts. As part of this review, the Branch is seeking recommendations and best-practice advice regarding intrusion detection solutions. Also, in 2006 the Branch will be acquiring an enterprise network management system to further enhance its network monitoring capabilities. Both of these initiatives will provide the required monitoring and controls for active network jacks in public boardrooms.

Passwords

Observation and Recommendation

We noted that during our review that the actual network password length is not in compliance with the City's security policies and procedures. Passwords are set at minimum 5 characters long, which is below the recommended value of 6 characters.

Weak password controls increase the risk of unauthorized changes to production data and/or dissemination of privileged information to intruders or unauthorized personnel.

Password standards should be enforced, a mandatory rotation (90-120 days) should be implemented as well as a permanent lockout after numerous failed attempts (3). Implementation of these controls will reduce the risk of unauthorized access and help to promote data integrity.

Management's Comment

The Network Account Management policy was reviewed in July 2005. The following settings relating to user account password management have implemented:

- minimum password length: 8 alphanumeric, upper and lower case characters for user accounts;
- minimum password lifetime: 1 day for user accounts;
- maximum password lifetime: 90 days for user accounts;
- failed login attempts before account is locked out: 3 for use.

SAP Parameters

Observation and Recommendation

Although observations were raised during the prior year audit, some SAP parameters remain unset at recommended values, and therefore represent potential security weaknesses.

Not setting these parameters in accordance with recommended practices compromises logical access controls. Weak logical access controls increase the risk of unauthorized system access. Unauthorized users with access to SAP can then impact the integrity of the data, confidentiality of information and the availability of the system.

- **rdisp/gui_auto_logout** – Number of seconds of idle time after which the user is logged out. Any value superior to 30 min (1800 seconds), increases the risk of unauthorized use of the computer. The current setting is 300 minutes (18000 seconds).
- **rec/client** – Flag activating the log file recording changes made to the tables of SAP. A good practice is to define this parameter with the client name or the value ON. In this case and depending on the table logged, the audit trail will be ensured. Currently this is off. Due to the performance issues associated with logging all tables, logging can be restricted to configuration tables that typically don't change frequently.
- **login/fails_to_session_end** – This setting determines the number of incorrect login attempts before the system ends the login attempt and requires the SAPGUI to be executed again. Currently, this is set to 6 attempts. The default is 3.

Management's Comment

Point 1 - rdisp/gui_auto_logout

This parameter is set at 300 minutes to meet operational requirements. Management feels there are two compensating internal control factors that eliminate the risk of unauthorized use of the system. The first control is the City of Ottawa's standard desktop configuration, which enforces a 15 minute screen saver password protection for computer idle time. The second internal control is the City's responsible computing policy Section 4.2 Unattended Workstations which states "users shall not leave a workstation unattended that is logged into the network without enabling a password screensaver."

Point 2 - rec/client

As mentioned in a prior Management Letter dated May 30, 2004, setting this parameter "will enable logging on all tables in a client. We have verified with SAP and there is no way to turn logging on for specific tables. It's done for the entire client, or not at all. SAP does not recommend complete logging as it has a major performance impact on a production system." As indicated above in your comments, configuration tables do not typically change frequently. The Support Center has transport procedures in place to ensure that all updates to configuration tables are documented, tested and approved prior to moving through the Production landscape.

Point 3 - login/fails_to_session_end

Management agrees. This parameter change was corrected on September 20th, 2004. However, this has appeared on this year's management letter, as the parameter change was not applied to all Production application servers. This was corrected earlier this year, and all environments now reflect the appropriate parameter amount of 3.