

APPENDIX 1

REVIEW OF MANAGEMENT AND OVERSIGHT OF THE INTEGRATED BUSINESS MANAGEMENT SYSTEM (IBMS)

January 16, 2009



Auditor General's Office

Jeffrey Griffiths, C.A., C.F.E.
Auditor General
City of Toronto

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
BACKGROUND	3
AUDIT OBJECTIVES, SCOPE AND METHODOLOGY.....	5
RESULTS.....	6
A. LACK OF A CORPORATE IBMS GOVERNANCE STRUCTURE	6
A.1. Alignment of Business and Information Technology Strategies	6
A.2. Lack of IBMS Risk Identification and Management	9
B. GENERAL INFORMATION TECHNOLOGY CONTROLS NEED STRENGTHENING	11
B.1. Performance Indicators for IBMS Do Not Exist.....	11
B.2. IBMS Business Continuity Plan Does Not Exist	11
B.3. Service Level Agreements	12
B.4. Concerns Related to IBMS User Training	13
B.5. Change Management.....	14
C. IBMS SECURITY MANAGEMENT PRACTICES.....	15
C.1. Lack of IBMS Security Management and Oversight.....	16
C.2. Review of User Access and Roles Required.....	16
C.3. No Formal Security Policies and Procedures	16
D. STRENGTHENING IBMS SYSTEM CONTROLS	17
D.1. Manual Processes and Data Entry Can Be Minimized By Integrating IBMS With the City's SAP Financial System	17
D.2. IBMS Data Not Archived.....	17
D.3. Non-Compliance With Vendor Agreement.....	18
D.4. Annual Savings Possible on System Maintenance Costs.....	19
E. OPERATIONAL CONTROLS.....	19
E.1. Lack of Proper Separation of Duties in IBMS Fee Revisions	19
CONCLUSION.....	20

EXECUTIVE SUMMARY

IBMS is critical for administering and enforcing the Municipal Code and City By-laws

Like many government organizations, the City of Toronto relies on large and complex information technology systems to support business operations. The Integrated Business Management System commonly known as IBMS is a critical City information technology system for administration and enforcement of the Toronto Municipal Code, many City of Toronto By-laws and the *City of Toronto Act*.

System processes annual revenues of approximately \$26 million

IBMS provides information technology support to many users throughout the City. Divisional users commonly rely on IBMS for automatically calculating fees, creating invoices and generating receipts. IBMS also provides a role in the billing and collection for annual revenues of approximately \$26 million.

In 2008, IBMS played a critical role in processing approximately 36,000 building permits, tracking over 91,000 building inspections, 3,589 City Planning applications and over 86,000 investigations.

IBMS maintains information on over two million people and 750,000 property records.

Recommendations in this report may have relevance to other information technology system applications

The recommendations included in this report may be relevant to information technology systems throughout the City and its Agencies, Boards, Commissions and Corporations and should be reviewed, evaluated and implemented as deemed appropriate.

Issues identified in previous audit reports

Over the past number of years, the Auditor General has issued several reports related to the management of the City's information technology assets including several on SAP. Some of the issues identified in this report are similar to those raised in these previous reports.

Key Findings

The information technology governance structure as it relates to IBMS requires review. While there is a certain degree of divisional coordination, the current governance approach is for the most part fragmented. The major focus in information technology governance relates to the level of Corporate management at which major IT decisions are made. Divisions should not be permitted to make independent decisions concerning information systems without considering Corporate goals and strategies.

The development of an effective IT governance structure will to a great extent address many of the other findings in this report which include the following:

- Need to strengthen coordination and oversight to ensure IBMS related resources provide expected results;
- Lack of a proper risk management program to identify and manage IBMS business risks;
- Lack of performance indicators to monitor and assess methods to improve service delivery;
- Lack of agreed upon service level agreements between user divisions to ensure IBMS provides the expected level of service;
- Lack of a comprehensive business continuity plan to ensure divisions can continue to function in the event of a disaster or system failure due to an unanticipated event;
- Need to improve change management practices to ensure changes are appropriately approved, documented and implemented in a systematic and controlled manner;
- A more practice approach to managing security is needed to ensure approved security policies are followed and compliance with general accepted security practices;

- Lack of integration between IBMS and the SAP Financial System;
- Lack of procedures or criteria for archiving information contained in IBMS;
- IBMS software contract needs to be managed better; and
- Lack of separation of duties with respect to updating Council approved fees.

This report contains 15 recommendations some of which may require additional resources while others require staff to reevaluate how IBMS can be used to enhance City services in a more effective and efficient manner.

The Auditor General issued a separate letter to management detailing certain not so significant issues that came to our attention during the audit. These issues related to reconciliation of financial records and harmonization of business practices.

BACKGROUND

A significant amount of confidential information is maintained on IBMS

City Planning, Toronto Building, and Municipal Licensing and Standards collect and record information related to the services they provide. A significant amount of this information is confidential. Examples of data collected and maintained include personal information and information concerning a citizen's building permit, planning application and circumstances related to compliance and other investigations conducted under the authority of the Building Code Act and the City of Toronto Municipal Code. This data is collected and maintained in an information management system called IBMS.

IBMS is used by over 900 staff in more than a dozen different City divisions

IBMS is an information management system developed to assist over 900 staff across more than a dozen different City divisions including City Planning, Toronto Building, and Municipal Licensing and Standards. Although each division has its own distinct mission and requirements, divisions have collaborated in developing, operating and maintaining IBMS as many of its functions are interrelated.

Information maintained in IBMS must be reliable, accurate and complete

Information maintained in IBMS is used for decision-making, by-law enforcement and revenue billing and collection. In order for City divisions to rely on this information it must be reliable, accurate and complete.

What is IBMS?

IBMS is a project tracking and data management system. It provides for automated business processes, activities and tracking. It allows for automatic assignment of tasks and modifications based on changing business needs. Common tasks accomplished using IBMS include amending user fees, billing and collection, maintaining project tracking records, producing status reports and assigning various tasks to City employees. Information is managed through reports designed to provide summaries to management. IBMS is also used to transmit City related reports to Statistics Canada and City Council.

IBMS supports key business services. In 2008, IBMS related transactions included:

Operational highlights

- Over 35,725 Building Permits issued (\$6.5 billion value);
- 91,138 Building Inspections;
- 634 Development Review applications processed;
- 86,888 Municipal Licensing and Standards investigations; and
- 2,955 Committee of Adjustment applications.

IBMS maintains over 720,000 property records and over two million individual client records.

Over \$8 million invested in IBMS since 1999 with plans for an additional \$2.7 million over the next four years

Since 1999 the City has spent over \$8 million on IBMS and other related information technology capital projects such as websites for Municipal Licensing and Standards and Toronto Buildings that are integrated into IBMS.

The 2009–2012 Capital Plan includes six IBMS related projects for a total planned cost of \$2.7 million.

AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

IBMS was selected for review and included in the Auditor General's 2008 Audit Work Plan based on the City's significant ongoing investment in the System as well as the potential risks associated with the System. From a potential risk perspective, IBMS is unique as it serves the business needs of multiple divisions. Unforeseen circumstances that result in the inability of IBMS to provide reliable service could have significant impact on the delivery of critical City services.

***Adequacy of
IBMS control
environment***

The overall objective of the audit was to determine whether the City's management and oversight of IBMS ensures the reliability, integrity and confidentiality of information produced and maintained by the System.

***Audit Scope
included
governance
framework and
general
information
technology
controls***

The audit scope included a review of the governance framework and information technology general controls to ensure appropriate system development and implementation.

Our audit scope also included a review of data files, reports and system controls.

The audit reviewed IBMS related transactions from January 2007 to May 2008.

***Audit
Methodology***

Our audit methodology included:

- A review of system controls;
- A review of IBMS related documentation;
- An analysis of data extracted from IBMS;
- Interviews with IBMS Information and Technology support staff and IBMS system users;
- A review of the 2000 Privacy Impact Assessment Report related to the capture, storage and release of personal information; and
- A survey of IBMS user satisfaction.

Compliance with government auditing standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

RESULTS

This section of the report contains findings from our audit work followed by specific recommendations.

A. LACK OF A CORPORATE IBMS GOVERNANCE STRUCTURE

“IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise’s IT sustains and extends the organisation’s strategies and objectives.”
(excerpt from IT Governance Institute, Control Objectives for Information and related Technology (COBIT®))

A.1. Alignment of Business and Information Technology Strategies

IBMS is used for administration and enforcement of the Toronto Municipal Code and other City By-laws

IBMS is a key City information technology system used for administration and enforcement of the Toronto Municipal Code, the *City of Toronto Act* and many City by-laws. Over 900 staff across more than a dozen different City divisions use IBMS. IBMS is an essential business tool for many divisions including City Planning, Toronto Building and Municipal Licensing and Standards.

A few examples of City IBMS users include:

Supports processing of planning applications, building permits, and tracks complaints and licensing and zoning violations

- City Planners process planning applications, generate public meeting notices and track legal agreements related to planning applications;
- Toronto building officials process building permit applications and zoning reviews, generate and track notices and compliance orders, and ensure compliance with application processing requirements, permit issuance and clearance;
- Municipal Licensing and Standards Officers use IBMS to maintain investigation files for complaints and potential licensing and zoning violations.

Integral part of day to day City activities

In short, it is a vital part of City business.

Lack of a proper governance structure

An important issue identified in our audit relates to the IBMS governance structure. Responsibility for the management and administration of IBMS is not well defined. Responsibility for various aspects of IBMS is distributed among the Information and Technology Division and IBMS business users in other divisions. Clear, mutually endorsed roles and responsibilities have not been established. Improvement in the IBMS information technology governance framework, strategic planning and leadership are required.

Governance structure provides leadership, organizational structure and processes to support City business objectives

Effective Governance Framework

Information technology governance is defined as the leadership, organizational structure and processes that ensure information technology extends and supports corporate business strategies and objectives. It is the core framework designed to align technology with business and should be designed to effectively and efficiently allocate resources, measure performance and manage risks.

A well defined governance structure is an important component of any information technology system, particularly where a system has many diverse and interrelated users throughout the City. In this context, the lack of a coordinated process has contributed to a number of situations where value for money has not been realized. Specifically, we have identified two instances where the lack of an effective governance process has been problematic. In both cases, there was little coordination or senior management direction in relation to the initiatives undertaken in the development of enhancements to IBMS.

Need for IBMS Governance Structure – Two Examples

After months of work and effort, project abandoned

The first example occurred in 2005. After months of work and effort by Divisional information and technology staff on IBMS to meet requirements specified by the Division, a decision was made to abandon the project and implement an alternative method to meet the Division's needs. In these circumstances, the resources used in the initial development were of no long term benefit.

Concerns over handling cash and payments not addressed in an efficient and timely manner

Another example of where a change in direction resulted in inefficient and wasteful use of staff resources was in relation to management's response to cash handling and payment concerns expressed in a 2005 report issued by the City Manager's Internal Audit Unit. At the time, management considered it a high priority to initiate a project to improve IBMS controls related to cash controls and payment processing.

After considerable work, another project deferred

After a considerable amount of work, the initiative was deferred. Three years later, in 2008 management decided again to resume efforts to address concerns raised in the report. In this case the change in direction resulted in cash control concerns not being addressed in a timely manner and any work performed during the original assignment would require repeating in the future.

Although management decisions should allow for flexibility, the examples provide evidence of the need for communication, coordination, and accountability in Corporate decision-making. Business user senior management should have some say in project decisions but these decisions should not be made outside the Corporate information technology governance structure.

Governance structure should allow for transparency, justification and accountability for management decisions

In March 2008, the City introduced an SAP governance structure. The SAP governance structure includes a steering committee which considers City priorities, proposed system initiatives, system implementation guidelines and provides project monitoring. The steering committee also provides periodic performance and monitoring reports to the City Business Advisory Panel and Enterprise Architecture Review Panel. A similar model does not exist for IBMS.

SAP Governance Model should be adopted for IBMS

Because IBMS supports multiple divisions, a well defined governance structure is required to ensure related system decisions do not result in wasted funds and inefficient use of resources.

Recommendation:

- 1. The City Manager in consultation with the Chief Information Officer give consideration to the establishment of an IBMS governance model which provides for senior management approval and prioritization of all IBMS related projects. The governance model follow the process recently established in relation to the development of SAP projects.**

A.2. Lack of IBMS Risk Identification and Management

A proper risk management program requires the user to identify potential risks and the Corporate information technology division to develop strategies to deal with user identified risks. From IT Governance Institute and Information Systems Audit and Control Association

Risk management is an essential management function

Corporate information technology resources are vulnerable to risk. Legal, security and environmental risks are just a few that need to be identified and managed. Managing information technology risk protects City resources and ensures reliable City services. Risk management is an ongoing management function and should determine where resources are directed to reduce risk.

IBMS is a key information technology tool which crosses divisional lines. In order for the Information and Technology Division to address IBMS system related risks, IBMS user divisions need to identify potential IBMS related risks.

***IBMS
information
technology risk
identification not
complete***

Divisions using IBMS have not identified related user risks. The lack of a proper IBMS risk identification and reduction program exposes the City to potential risks. Divisional responsibilities and risks related to IBMS should be formalized so divisions are aware of their respective responsibilities. Business continuity, privacy and unauthorized system access are a few examples of IBMS related risks.

Two examples of risk strategies might include action required by user divisions and Information and Technology staff in the event of an IBMS system failure for an extended period, and strategies for encrypting data to ensure privacy in accordance with Corporate Access and Privacy requirements.

The Corporate information technology risk assessment should:

- Evaluate, prioritize and document the impact of potential risks;
- Describe risk reduction methods; and
- Provide for technology and business practice changes and updates.

Understanding specific risks associated with IBMS and other computer systems allow management to take appropriate steps to ensure system reliability, security and continuity are not compromised. The lack of a formal process to understand and respond to factors leading to an information system failure increases business continuity risk.

Recommendation:

- 2. The City Manager in consultation with the Chief Information Officer require that divisions identify business risks relating to the IBMS Information Technology System. The Chief Information Officer review all such risks and ensure strategies and processes are in place to address all such risks.**

B. GENERAL INFORMATION TECHNOLOGY CONTROLS NEED STRENGTHENING

General controls are the structures, policies and procedures that apply to the overall information technology activity. General controls create the IBMS control environment.
From IT Controls Guide, Institute of Internal Auditors (IIA) IT Controls Guide.

B.1. Performance Indicators for IBMS Do Not Exist

***What gets
measured, gets
managed***

Information technology performance should be monitored regularly. This process includes defining relevant performance indicators, systematic and timely performance reporting, and prompt action on deviations. Monitoring provides a way to progressively improve and maintain quality of service. In short, what gets measured gets managed.

***Performance
indicators do not
exist***

IBMS performance measures related to efficiency and effectiveness do not exist.

Examples of relevant IBMS performance measures might include responding to urgent help desk requests within a specified period of time, responding to non-urgent help desk requests within a specified time, and processing security access requests within a given time.

Recommendation:

- 3. The City Manager in consultation with the Chief Information Officer and divisions develop IBMS performance measures. Such measures be used to monitor ongoing performance. Where performance does not meet such measures, corrective action be taken.**

B.2. IBMS Business Continuity Plan Does Not Exist

A Business Continuity Plan provides the framework for a controlled response and recovery from unanticipated events that threaten service reliability.

***IBMS is
considered
"Super Critical"
and "Critical" to
Divisions***

According to a 2007 consulting report related to Business Continuity Planning, City Planning and Toronto Building Divisions consider the use of IBMS as "Super Critical" and "Critical" to their operations.

Divisions are not adequately prepared in the event of an extended unanticipated system failure

Divisions using IBMS do not have a comprehensive Business Continuity Plan in the event of an unanticipated system failure. Initiatives to deal with technology aspects such as ensuring appropriate computer systems are available, are on hold pending the outcome of the City's Information Technology Governance and Transformation process. Any plans that do exist are informal and inadequate.

Business continuity plans are the responsibility of the business user

Business continuity plans are the responsibility of the business user and as such divisional management takes ownership over ensuring a comprehensive plan, including the information technology component, is developed, maintained and tested.

In the event of an unanticipated system disruption, divisions using the system will likely experience an uncoordinated recovery effort, resulting in inefficiencies and an extended recovery time.

Central oversight and a coordinated systematic approach in planning for disaster recovery strategies do not exist.

Recommendation:

- 4. The City Manager and Chief Information Officer as part of the IBMS governance process give priority to the development of IBMS business continuity plans. Such plans should include disaster and recovery planning.**

B.3. Service Level Agreements

Service level agreements define service expectations

A service level agreement is a contract between the service provider and divisional users. Service level agreements define expected services and service levels.

For IBMS, the Information and Technology Division is the service provider. Operational divisions using IBMS are system users.

Service level agreements do not exist

Service level agreements between the service provider and the divisional users do not exist. Although such agreements do not prevent delays or poor quality of service, they do provide a framework for establishing performance expectations and corrective action when needed.

Leads to user dissatisfaction and frustration

In our survey of IBMS users, certain responses noted instances where expectations in service delivery related to system training and timely response to service requests were not met. These two areas are among many others that should be provided for under a properly administered service level agreement.

Recommendation:

- 5. The City Manager in consultation with the Chief Information Officer develop and formalize service level agreements for information technology services provided to City Divisions by the Information and Technology Division.**

B.4. Concerns Related to IBMS User Training

Challenges in delivering IBMS training

Based on the results of our IBMS User Survey, training challenges facing the City include:

- integrating employee daily use of IBMS with daily business activities;
- anticipating divisional training needs; and
- turnover of staff trainers.

Divisions have some flexibility to take training when needed

Training materials have been developed and are available online to city staff. Online training provides divisions with scheduling flexibility. Feedback from interviews and 6 of 24 survey respondents indicated a need for strengthening IBMS related training in the following areas:

- concern related to the overall quality and range of training;
- concern over training material; and
- training concerns related to the balance between IBMS “technical” features and daily “business use” features.

Lack of user input into training material

We were also informed that improvements could be made in allowing for user input into training material to ensure information is complete and correct, and ensuring that training links to the user's daily business activity.

Inadequate IBMS training leads to poor user acceptance, frustration, an increased burden on the “Help Desk” and improper System use.

Recommendation:

- 6. The City Manager in consultation with the Chief Information Officer review current levels of training available to IBMS users, and solicit input from divisional users in relation to training effectiveness. Deficiencies in regard to training identified by users be appropriately addressed.**

B.5. Change Management

***System changes
need to be
managed
carefully***

An effective change management strategy provides systematic implementation of planned or urgent changes to IBMS. An effective change management strategy supports a cost-effective approach to system changes ensuring user requirements are cost justified, prioritized and approved.

Change management is more challenging in an environment where the system undergoing change supports multiple divisions. IBMS is a modular system supporting operations in several divisions. Proper change management ensures system integrity is maintained through user acceptance testing and authorization prior to transition from “testing” to a “live” system.

Improvements are needed to IBMS change management practices. For example:

- IBMS technical documentation and related changes are not retained in a central location. Technical documentation is critical to divisional operations and should be accessible. Without proper storage, IBMS related information may be misplaced, lost or discarded.
- IBMS produces many reports for user divisions. These reports are changed periodically to be made more useful and relevant to users. Generally accepted industry guidelines recommend management approval of system changes before released for use. Management approval of changes ensures accuracy, completeness and relevance.

Changes to IBMS reports do not receive management approval. Failure to obtain management’s approval increases the risk that reports will be inaccurate, not relevant or incomplete.

- System program developers have access to the “live” production database and a limited number of transactions are tested in the “live” database. These practices present significant IBMS security risks and are not in accordance with generally accepted industry practices for maintaining data security and integrity.

The Information and Technology Division has implemented a change management protocol for SAP. This protocol is followed when changes to SAP are required. The protocol includes:

- Documentation standards;
- Documentation storage requirements;
- Management authorization of proposed changes;
- Respective roles of Information Technology staff and user divisions; and
- Separation of duty guidelines for system developers and user divisions.

A similar model does not exist for IBMS.

A proper change management protocol will ensure divisional users and Information and Technology staff efforts are coordinated.

Recommendation:

- 7. The City Manager in consultation with the Chief Information Officer develop and implement a change management protocol for IBMS. Such a protocol take into account the SAP change management protocol.**

C. IBMS SECURITY MANAGEMENT PRACTICES

The protection of data processed by IBMS is critical to ensuring data integrity is maintained and safe from unauthorized access. Although there are various layers of security in place to protect the City’s data, this report focuses on IBMS security practices. These practices include establishing and maintaining security roles and responsibilities, policies, standards and procedures, performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses.

C.1. Lack of IBMS Security Management and Oversight

More effort is required in managing overall security practices. The absence of a proactive oversight activity increases the risk that certain security activities such as monitoring user activity, documenting security rules and monitoring for compliance with good security practices may not be performed.

Recommendation:

- 8. The City Manager in consultation with the Chief Information Officer develop security plans, standards and related staff responsibilities for managing and overseeing IBMS security.**

C.2. Review of User Access and Roles Required

Various IBMS users fulfill unique roles and are provided different system access rights. Depending on the need and role, users are granted various levels of ability to view, add, change or delete IBMS data.

Periodic review and removal of non-active users is not performed. Regular review of IBMS system use assists in deactivating dormant accounts and reduces the risk of unauthorized system use. Sixteen percent of “active” IBMS users had not accessed the system for one to three years.

Recommendation:

- 9. The City Manager in consultation with the Chief Information Officer be required to conduct periodic reviews of current IBMS user security to ensure access is compatible with user roles. Such review should also include an analysis of the last date of use. Dormant users should be eliminated from system access.**

C.3. No Formal Security Policies and Procedures

There are no formally approved security policies and procedures for adding, changing or deleting IBMS users. The lack of formal security policies and procedures increases the risk of unauthorized access to the system and erodes user accountability.

Recommendation:

- 10. The Chief Information Officer develop formal written procedures for granting, changing or removing IBMS user access.**

D. STRENGTHENING IBMS SYSTEM CONTROLS

D.1. Manual Processes and Data Entry Can Be Minimized By Integrating IBMS With the City's SAP Financial System

No integration with City's SAP Financial System

Implementation of the City's SAP Financial System brought with it expected efficiency gains through integration with other major systems such as IBMS. Currently there is no electronic interface between these two systems.

Current process inefficient with added risk of human error

The lack of an electronic interface means information must be manually extracted from IBMS, then manually entered into the City SAP Financial System. In addition to the inefficiency of manually entering data from one system to another, there is increased opportunity for human error. Data entry errors are avoided if information is electronically transferred from one system to the other.

Recommendation:

- 11. The City Manager and Chief Information Officer develop as a priority an electronic interface between IBMS and the City's SAP Financial System. Such an interface would reduce the requirement for manual analysis and processing.**

D.2. IBMS Data Not Archived

Data retention requirements governed by the City's Records Retention By-law

In accordance with the *City of Toronto Act*, the City is responsible for the identification and retention and/or disposition of all records. Records may not be destroyed unless a schedule for their destruction has been approved by Council in the form of a records retention by-law.

The City Records and Information Management Division creates and maintains retention schedules and by-laws based on each business unit's requirements and plan. The Division also oversees the systematic transfer and destruction of records no longer needed.

IBMS records created since 1999 still reside in the System

All IBMS data created since inception in 1999 is still maintained in the System. Records created through the use of IBMS are not archived nor are there policies and procedures outlining when and how records should be archived. Allowing the volume of records to increase requires more storage space, increased costs and can impact system performance.

Recommendation:

- 12. The City Manager in consultation with the Chief Information Officer and City Clerk review the record retention policy for all IBMS related records. Such a review include the establishment of policies and procedures for archiving IBMS records.**

D.3. Non-Compliance With Vendor Agreement

City does not have a copy of IBMS source code as stipulated in the agreement

The agreement between the City and the System software vendor states that the vendor is contractually obligated to provide the City with a copy of the System source code within 15 days of issuing each new software release. This is to allow for City staff to make software modifications in the event the vendor fails to perform obligations provided in accordance with the contract. The City does not have a copy of the source code as stipulated in the contract.

Recommendation:

- 13. The Chief Information Officer obtain a copy of the System source code for the current release of the System software and ensure future releases are accompanied with System software under the terms of the agreement.**

D.4. Annual Savings Possible on System Maintenance Costs

The maintenance agreement between the City and the System software vendor specifies annual maintenance costs. Annual maintenance costs are based on the number of licenses purchased.

Subsequent to the City's purchase of software licenses, Toronto Public Health purchased a number of software licenses from the same vendor.

Toronto Public Health is paying higher license maintenance costs for software also used by the City. If Toronto Public Health software maintenance costs were based on the rate applicable to the City's software licenses, an annual savings of approximately \$36,000 would be realized.

Recommendation:

- 14. The City Manager conduct a review of related System users in the City and its Agencies, Boards and Commissions and update the existing software maintenance contract as required.**

E. OPERATIONAL CONTROLS

E.1. Lack of Proper Separation of Duties in IBMS Fee Revisions

Fees for services are revised annually

Each year, fees for services provided by City Planning, Toronto Building, and Municipal Licensing and Standards Divisions are reviewed and revised. After Council authorization to revise fees, appropriate revisions are made in IBMS.

Technical support staff update fee changes

Generally accepted control practices require the business user to perform the procedure for revising fees supported by IBMS. This is to ensure proper separation of duties. We noted in our review that the process for revising fees is conducted by technical support staff. This practice is not in accordance with generally accepted practice.

Undocumented Fee Revisions

In addition, methods used by technical support staff in making fee revisions were inconsistent among staff members and in some cases undocumented, leaving no audit trail.

Recommendation:

- 15. The City Manager ensure staff from business units perform the procedure for revising service fees maintained in IBMS and that the process be appropriately documented.**

CONCLUSION

For IBMS to serve the City efficiently and effectively improvements to management and oversight are required. The establishment of an IBMS information technology governance structure will go a long way in helping to coordinate IBMS related decision-making and change management. Implementation of a long range strategic plan, performance measures and a business continuity plan will also ensure coordinated growth and development for system users and ensure reliable service to IBMS user divisions.

A number of other areas can be further improved including:

- User training
- Change management
- Security management and oversight
- System Controls including SAP interface and data archiving
- Software licensing
- Contract management
- Operational controls

Ongoing management, monitoring and oversight of IBMS related resources are essential in maintaining reliable service to user divisions and the public.