Office of the Auditor General

Audit of Information Technology Risk Management

Tabled at Audit Committee – November 26, 2015

Contents

Executive Summary

Introduction

The City of Ottawa's Audit Plan for 2014, as approved by Council in March 2014, included audits of Information Technology (IT) and related investments. This Audit of IT Risk Management, along with an Audit of IT Security Incident Handling and Response, were completed in accordance with the 2014 Audit Plan.

Background

Throughout the City, IT-based solutions and innovations have supported the achievement of a variety of operational and strategic objectives. The role of technology is expected to continue a steep growth pattern as new and innovative solutions are developed. However, while there are opportunities for IT to support the City's strategic objectives, there are a variety of traditional and emerging IT risks that must be considered and effectively managed at the highest level.

For an organization of the complexity and size of the City of Ottawa, the breadth and depth of potential IT-related risks is significant. Whether it's maintaining operational or administrative capabilities, protecting valuable or sensitive assets, supporting compliance or enabling achievement of business or strategic imperatives, there is an inherent risk relating to IT in nearly every City activity or function. As such, while there is obviously a technical element of IT risk, business managers from across the City are ultimately the most important stakeholders in the management of IT risks.

The City's Approach to IT Risk Management

The Enhanced Risk Management (ERM) Framework

In 2010, Council approved a conceptual Enhanced Risk Management (ERM) Framework and Enhanced Risk Management Policy. By 2011, the Framework had been implemented across the City. The Framework outlines roles and responsibilities for risk management, the City's risk management process, and provides other resources and tools for departmental managers and others with responsibilities under the Framework and Policy. Since 2011, City departments have annually conducted risk analysis activities which have led to the development of the Corporate Risk Profile (CRP).

IT Risk

IT risks are those associated with the use, ownership, operation, involvement, influence and adoption of IT within an organization. It consists of IT-related events that could impact the organization's ability to achieve its goals and objectives. Like most risks, they can occur with uncertain frequency and magnitude. Examples of IT risks include the loss/corruption of information assets, and the inability to provide IT-dependent business functions.

IT Risk Management Framework

The management of IT risks is supported through a number of policies, processes and practices at both an enterprise-wide and at a more granular level (e.g., at the IT project level or incident response level). At the enterprise level, IT-related risks are explicitly captured within the ERM Framework. While the Information Technology Services (ITS) Department is the single most significant source of IT risks, IT risks were identified by 65% of all departments in 2014.

The ITS Department plays an important role in the management of IT risks at the project and systems level. In addition to providing training/awareness sessions related to IT risks, ITS is responsible for developing IT related policies and guidance to support the management of IT risks.

ITS has a formal and broad responsibility for the management of IT risks, however, there are independent IT groups that serve in a few departments where one or more business applications or systems that, while often connected to enterprise architecture, operate fully or in part, autonomously from ITS. These include Transit Services Department, Traffic Operation Branch, Drinking Water Services Branch and Wastewater Services Branch.

Audit Objectives and Scope

The overall objective of this audit was to provide an independent assessment relating to the adequacy and effectiveness of the City's IT Risk Management governance, policies, practices and procedures. Three (3) specific audit objectives were considered:

Objective No. 1: Assess if IT Risk Management Governance at the City effectively supports management of the City's IT-related risks.

Objective No. 2: Assess if the City's IT Risk Management Framework of policies, practices and procedures are adequately designed and aligned with the City's ERM Framework.

Objective No. 3: Assess if the City's IT Risk Management policies, practices and procedures are effectively supporting the identification, evaluation, mitigation and monitoring of IT risks across the City.

The scope of this audit included IT risk management activities across the City of Ottawa. It involved an examination of both the design and effectiveness of controls (policies, practices and procedures). We reviewed roles, responsibilities and accountabilities as they exist both within ITS and across all City business lines and departments that use IT. This included an examination of IT risk management in areas where independent technology groups exist.

Summary of Key Findings

Governance, Executive Leadership and Support

The City has a strong committee structure for addressing IT risk management. Following the Audit of IT Governance, tabled in March 2015, the reporting structure was strengthened, although this audit noted areas where improvement was required.

The City has experienced a high rate of turnover in the Director, ITS and Chief Information Officer (CIO) position over the past few years including extended periods where the position was occupied by a temporary replacement. A new Director, ITS and CIO was hired in the spring of 2015. We noted, that the ITS Staff interviewed as part of this audit were positive and enthusiastic regarding the new CIO’s leadership, strategic direction and support.

Notwithstanding this positive development, the City has yet to develop a comprehensive Governance component of an Information Technology Risk Management (ITRM) Framework including clear and consistent responsibilities and accountabilities for City executives and management embedded in an ITRM Framework. In particular, the effectiveness of the existing ITRM Governance is impacted by several factors including:

a) Absence of an ITRM Framework with a comprehensive Governance component;
b) The method of prioritizing, selecting and funding IT initiatives;
c) Authority of Corporate Information Technology Management Team (CITMT); and
d) Authority of the CIO.

Each of these issues are discussed further below.

Governance Component to an ITRM Framework

While the City does have some components of an effective ITRM Framework embedded in the ERM, there is no stand-alone ITRM Framework with governance capable of supporting a mature risk culture. Effective governance within an ITRM would help to provide clear guidance on the City’s IT risk appetite and IT risk tolerance as well as oversight on their application. Without clear direction and oversight on these key components, it is not possible to develop an effective ITRM Framework (refer to the next section, entitled “IT Risk Management Framework Design and Alignment” for additional discussion of ITRM Framework).

Prioritization and Funding of IT Projects

IT projects are brought forward for consideration by individual departments. Departments are required to identify each project's source of funding and are encouraged to only bring forward funded projects. Notwithstanding instances where unfunded projects have been identified and approved as priority investments, this approach means that approved projects may not always be aligned with corporate priorities.

There is little flexibility for required adjustments to the ITS infrastructure budget and/or other departmental budgets for high priority IT projects as a large portion of IT budgets are controlled by individual departments, not ITS. Some departments (Transit, Traffic, and Water) have large IT budgets and independent IT groups. These budgets are typically based on historical requirements which have then become part of their baseline budget. This scenario supports the continued investment in IT risk management within some departments while IT deficiencies and related risks in other business lines are not addressed.

In addition, there are a variety of funding mechanisms, often with specific constraints. For example, the water and sewer surcharge funding can only be used for very specific water and sewer related activities.

Therefore, there is a significant risk that high priority IT risks are not being adequately addressed on a timely basis if funding is not readily available to the business owner. This applies to ageing IT infrastructure owned by ITS as well as new and existing initiatives owned/managed by independent groups such as Water, Transit, Traffic and other Information Management/Information Technology which belongs to other departments.

Authority of CITMT

While the concept of the Corporate IT Management Team (CITMT) approval process is sound, the process is hindered by the process described earlier whereby projects submitted to CITMT for consideration in the annual corporate IT plan are typically only those which are already funded. Funding may be sourced from individual departmental budgets, external sources such as the Province of Ontario, or with "earmarked" funding. As such, the funding status of IT projects, rather than a City-wide and risk-based priority ranking system, is a significant factor in determining which projects are considered by CITMT for inclusion in the annual corporate IT plan.

This decentralized approach to funding IT projects and absence of a City-wide priority ranking system impacts the effectiveness of CITMT's authority relative to its mandate. Specifically its mandate is "to plan, provide oversight and strategic direction necessary to:

- Deliver an annual corporate IT plan with a clear connection to the Corporate Strategic Plans as approved by council and its boards;
- Represent individual departmental and corporate needs;
- Support ITS in delivering on its mandate to provide innovative and cost effective technology solutions to deliver maximum business value;
- Base decisions on corporate strategic plan."

CITMT terms of reference also state that "CITMT serves as the corporation's primary agent of technology direction, having been given the authority by the Executive Committee to exercise leadership when undertaking its roles". While not explicitly stated in the terms of reference, CITMT has an implicit responsibility for leadership in recommending a corporate IT plan that is reflective of risk-based IT priorities across the City. CITMT's authority to discharge this responsibility is hindered by the current IT project funding model as well as the City's existing capability to identify and prioritize City-wide IT risks as discussed later in this report. As a result, decisions made regarding IT investments/expenditures may not always be aligned with overall corporate priorities and/or risk management objectives.

Authority of CIO

The job description for the Director, ITS and CIO position (both roles are performed by the same position) states that, in addition to directing the operations of the ITS department, from a corporate perspective the CIO is to provide strategic leadership for planning and implementation of a broad range of business and enterprise IM/IT initiatives, to support the City's service delivery objectives.

The position is to play a major leadership role in organizing, managing, and strengthening a comprehensive IT/IM infrastructure that will support and transform the administrative and service delivery areas of the City, and support its mandate. As well, the position is to oversee the implementation of departmental strategies, conduct long range fiscal planning with respect to IT and IM and serve as senior advisor regarding IM/IT issues to Council, Committees of Council and Counsellors to disseminate strategic direction, advice and technical information.

However, the CIO's actual ability to influence and manage is limited as staff responsible for IT in various departments and agencies (e.g. Ottawa Public Health, Transit, Water, Wastewater, etc.) are not functionally accountable to the CIO and lines of authority are not always clear. Further, the audit team was not able to identify any clear and formal description, in the job description or otherwise, of the CIOs authorities or responsibilities regarding the City-wide IT risks.

The lack of clarity around the authority of the CIO impedes his ability to:

- Promote a culture that supports ITRM objectives including influencing change at an executive level and introducing IT change management throughout the City and influencing/managing City-wide spending related to IM/IT;
- Align City-wide IT funding with the highest priority City-wide IT strategic initiatives;
- Tackle the highest priority City-wide IT risks on a timely and strategic basis; and
- Ensure compliance with policies, procedures and enforce central reporting of ITRM activities.

The reporting structure to and from the CIO is not consistent with best practises. The *RISK IT* framework recommends that the CIO position be responsible for all City-wide processes including Risk Governance, Risk Evaluation and Risk Response and that all subordinate IT management roles report to the CIO.

This would enable the CIO to both inform and advise the City Manager, who would have ultimate accountability for managing IT risk including funding of mitigation strategies and opportunities, as the CIO would control and answer for all IT related staff. It would also enable the CIO to better influence decisions to ensure that overall corporate priorities, such as maintaining the integrity of existing infrastructure and ensuring security receive the appropriate priority and related funding.

Ultimately however, to truly manage IT risk, and act on the opportunities which will transition the City of Ottawa into a leading “smart city, the CIO should have the authority, resources and ability to perform all the following:

- Manage Costs – Control the impact of IT spend on the enterprise;
- Keep the lights on – Ensure the IT and security needs are up and running;
- Act as an information broker - Provide insight to support business decisions;
- Generate ideas and solutions – Enhance business processes by being an active business partner;
- Deliver transformation – Prepare and develop the organization for change; and
- Bring business model innovation – Shape the future of the business with the right technology.

IT Risk Management Framework Design and Alignment

The City has yet to develop a comprehensive IT Risk Management (ITRM) Framework. While there are a variety of ITRM activities occurring (e.g. at the project and system level), as noted for Objective 1, the City has no clearly defined ITRM framework that serves to bridge the gap between ERM and more granular ITRM.

ERM processes are continuing to mature, including the relatively new and developing explicit classification of IT risk categories. Specifically, in 2015 the Technology Risks were changed from ten sub-categories, that were difficult to differentiate among, to six very different types of sub-categories – (1) Maintenance and Lifecycle, (2) Resource Unavailability, (3) Service Disruptions or Losses, (4) Social Media, (5) Software and Hardware renewal and (6) System failure. The new Technology risks provide much better alignment with types of IT risks than before and will provide clarity for grouping these risks moving forward.

However, while the City recently started identifying specific IT risks and embedding them in the ERM framework, there are many deficiencies in the documentation to support the identification, assessment and mitigation of IT risks. In particular, the design effectiveness of the existing ITRM framework is reduced by several factors including:

- Insufficient documented and approved ITRM framework with a supporting policy and procedures suite;
- Insufficient processes for the identification and assessment of City-wide IT risks;
- Weaknesses in challenge mechanisms for assessment of proposed/possible corrective measures;
- Insufficient training of ITS staff, IT professionals outside ITS and others who are non-IT professionals yet are tasked with performing IT risk assessment;
- Undocumented IT risk universe that would serve to support oversight and inform decision-makers; and
- Incompleteness of Business Technology Plan including how the plan is based on mitigating the highest risks/priorities as well as related timelines, costs and sources of financing.

Given the low maturity level of most City departments for ITRM and the broad and technical nature of IT risks, procedures and guidance at both the corporate and departmental level are not sufficient to ensure that the identification, evaluation, communication, mitigation, and monitoring of the most important IT risks is consistent, appropriate and timely. In addition, IT issues and priorities that are critical to City-wide objectives do not necessarily rise to the top.

These issues are discussed further below.

ITRM Framework – Responsibilities and Accountabilities

Responsibilities for those providing input to ITRM documents such as risk registers are not fully developed, beyond completion of the Corporate Risk Profile as part of the ERM process.   We would have expected to find clear, and consistent responsibilities and accountabilities for all employees involved in the ITRM process, including a RACI (Responsible – Accountable – Consulted – Informed) type model embedded in an ITRM

Framework with a supporting policy suite and processes. As noted earlier in this report, leading practises developed by ISACA were used to assess the effectiveness of the City's ITRM. Specifically **Responsibility** (those who must ensure that the activities are completed successfully) and **Accountability** (those who own the required resources and have the authority to approve the execution and/or accept the outcome of an activity) within specific *RISK IT* processes were assessed. These deficiencies in the City's ITRM framework impact the City's ability to:

- Integrate the management of IT risk into the overall ERM, thus allowing risk-return-aware decisions;
- Ensure there is an effective challenge mechanism to support both completeness and accuracy of the risks identified and the assessments of impact;
- Make well-informed decisions about the extent of the risk, and the risk appetite and risk tolerance of the enterprise, and
- Understand how to respond to the risk.

Policies and Procedures

Existing corporate level policies and procedures, including the Information Risk Management Policy, are consistent with the ERM Framework, however there is limited guidance or formal controls for departments, including those with independent IT groups, on their authority or responsibilities when engaging in activities that may impact the City's IT risk profile. Existing policies focus primarily on security threats and breaches of confidentiality of information, such as the Responsible Computing Policy or the Technology Devices Policy. However, there is a lack of policy guidance around other IT-related risks such as Use of Cloud-based or other 3rd party systems or services.

In addition, most departments:

- Have not developed their own policies, processes/procedures which reflect their unique IT risks, business objectives and environment; and,
- Rely on the annual ERM processes, ITS intervention, and/or potentially limited scope activities (e.g. Vulnerability Assessments - VAs) to address IT risk management.

Training and skill sets

The City conducts user training for IT systems and IM applications. However, while there is a large focus on security, there is a lack of training concerning the efficient use of IT resources.

In some business units, people who have little or no technical training are being tasked, under the ERM Framework, with the identification of risks and/or related mitigation strategies. As a result, there are gaps and weaknesses in the identification, assessment and mitigation of critical IT risks (security, confidentiality, integrity, availability, reputational, operational, compliance/legal, strategic, business continuity, etc.).

City-wide Business Technology Plan and ITS Strategic Plan

The2011-2014 ITS Strategic Plan outlines how ITS will support the previous Term of Council Vision by providing information on strategic objectives and related ITS initiatives, and how they tie with the City's strategic priorities. While it includes brief details of ITS' strategic initiatives including ownership, description and performance measures, it is limited in scope insofar as it presents a departmental view rather than a City-wide view of the City's IT strategy.

The Business Technology Plan (BTP), however does provide a City-wide view. The BTP provides a summary of planned activities including those related to ServiceOttawa, new projects, ongoing business initiatives and operational support. The audit team reviewed documentation (project charters, storyboards, risk assessments, change management strategies, and implementation plans, etc.) for three (3) IT projects in the BTP. While not all projects demonstrated a clearly documented linkage to corporate priorities, the most recently completed of the sample did include a clear reference to Council priorities and how the project would service to support these priorities. It will be important, going forward, that such linkages are consistently demonstrated.

IT Risk Universe

The process of identifying IT risks is first impeded by the absence of a full inventory of the IT universe across the City (applications, business owners, networks, interdependencies, etc.). In addition, there is no complete risk register (risks, impact, mitigation strategy, and status, etc.) that is developed with input from trained and qualified IT professionals.

This is a significant risk as there are several departmental IT groups which operate fully or in part independently from ITS (e.g. within Water, Wastewater, Transit, and Traffic). In addition to these independent IT groups, some departments operate applications which are not within the City's direct control (e.g. provincially mandated applications used by Ottawa Public Health). Further, there are a number of examples where business lines have acquired third party applications and/or leveraged cloud-based solutions for their business without ITS's involvement. Such applications inherently present IT risk to the City to the extent they are accessed via City computers, use City networks, and/or are otherwise connected to the City's IT infrastructure. This risk is potentially high, particularly where such applications contain personal and/or confidential information of the citizens of Ottawa.

In addition, there are legacy systems which continue to operate and rely on ageing IT infrastructure. These systems typically place considerable demand on resources responsible to support the ongoing operation and maintenance of these applications and related IT infrastructure.

Without a documented, complete and comprehensive inventory of all IT components and applications relying on the City's IT infrastructure, it is not possible to build a comprehensive risk register which identifies the IT risks, potential impact and required mitigation/corrective action.

IT Risk Management Approach Effectiveness

The issues related to governance and design noted earlier have significant implications on the effectiveness of ITRM across the City. While the ERM and Corporate Risk Profile processes and policies are followed and IT risks are routinely identified, evaluated and mitigated through the ERM or other activities, the following concerns exist regarding the completeness and quality of the final product:

- There is neither the culture nor capacity to support a complete and holistic view of IT risks and the effective management of these risks;
- Outputs may not have been subject to sufficient analysis, consideration and challenge by people with appropriate and sufficient skill sets/competencies to effectively perform this function;
- Some IT related issues may not be appropriately identified, assessed and subsequently escalated to both inform (awareness) and mitigate (plans and funding);
- It is not clear if all risks related to ageing infrastructure, data storage, network capabilities, etc. have been identified; and
- There is not always a linkage between the identification of a critical risk with the provision of sufficient resources allocated for effective mitigation.

For example, analysis of the IT category in the Corporate Risk Profile (CRP) revealed very little/no identification of some IT specific risks such as those raised in the Security Incident Handling report including out-sourcing, 3rd party software, cloud computing, oversight of IT vendors, disaster recovery/business continuity, software license management, end user computing, IT infrastructure loads and costs for IM demand.

Without a complete and comprehensive IT risk universe, there cannot be a common view of IT risks and the City cannot make risk-aware decisions. That is, the City cannot make decisions that consider the full range of opportunities and consequences from reliance on IT for success. As importantly, it is not possible for City staff to have a full understanding of all potential IT risks within the IT universe. That is, City staff, especially

ITS, do not know what risks they are not aware of, and cannot anticipate what corrective measures are required.

Recommendations and Management Responses

Recommendation 1

That the City Manager develops a robust Governance component of an ITRM Framework which:

- **Is aligned to the ERM Framework.**
- **Includes clearly defined roles, responsibilities, and authorities of City Executives and Management.**
- **Clearly establishes the basis for a corporate risk culture, including risk tolerance and risk appetite guidelines.**
- **Ensures that all mitigation strategies for risks identified as being above acceptable tolerance levels are considered for inclusion in the Annual Corporate IT Plan based on risk/priority, regardless of whether there is pre-approved funding identified.**

Management Response

Management agrees with this recommendation.

The City Manager will work with ITS and the Corporate Programs and Business Services department to develop a robust Governance component of an ITRM framework. Work done to implement this recommendation will be completed in conjunction with work being done to implement Recommendation 5. This recommendation will be complete by Q4 2016.

Recommendation 2

That the City Manager and City Treasurer undertake an assessment of IT spending to explore alternative funding models which will provide better alignment between mitigation of prioritized City-wide IT risks and funds available/provided and provide long term savings through improved, targeted IT spending.

Management Response

Management agrees with this recommendation.

The City Manager, CIO and City Treasurer will work to identify and implement a budgeting/funding model that will allow for the funding of risk items that are deemed unacceptable. This funding model will form a part of the ITRM framework referenced in Recommendation 5. This recommendation will be complete by Q2 2016.

Recommendation 3

That the City Manager take steps to strengthen the effective authority of CITMT including expanding reviews to include all City-wide IT risks and proposed/recommended mitigation strategies.

Management Response

Management agrees with this recommendation.

The City Manager, in conjunction with ITS will take steps to strengthen the effective authority of CITMT as part of the work being undertaken to implement Recommendation 1. Processes will be developed to incorporate the role of a senior oversight body in the risk mitigation decision-making process. This work will be completed by Q4 2017.

Recommendation 4

That the City Manager take steps to strengthen and confirm the role, responsibility and accountability of the Director, ITS and CIO position including consideration of alignment with the best practices identified in the ISACA *RISK IT* Framework as well as functional reporting of all City departments and agencies to the CIO for all IT matters.

Management Response

Management agrees with this recommendation.

The City Manager will take steps to strengthen and confirm the role, responsibilities and accountabilities of the Director, IT and CIO. In addition, as part of work done to implement Recommendation 1, the City Manager will consider best practices as identified in the ISACA RISK IT Framework in determining appropriate functional reporting for IT matters. This recommendation will be complete by Q4 2016.

Recommendation 5

That the CIO develop a robust ITRM Framework which:

- **Is aligned to the ERM Framework;**
- **Incorporates the recommended Governance component of an ITRM framework (Refer to recommendation #1);**
- **Includes clearly defined roles, responsibilities, and authorities for all City employees involved in ITRM;**
- **Incorporates a well-documented audit universe/inventory and a risk register;**
- **Incorporates a well-developed challenge mechanism conducted by trained and qualified IT professionals;**

- **Ensures that all mitigation strategies for risks identified as being above acceptable tolerance levels are communicated to Senior Management in a comprehensive and effective manner.**

Management Response

Management agrees with this recommendation.

The current ERM framework will be reviewed and the ITRM framework will be enhanced to include the policies, processes and authorities for the entire corporation. Risk tolerance guidelines will be developed to include the process whereby unacceptable risks will be escalated to the appropriate authorities. The annual budgeting exercise will include a risk mitigation component where unfunded risk reduction costs will be identified. This recommendation will be complete by Q4 2017.

Recommendation 6

That the CIO, in conjunction with the development of the ITRM Framework, develop a supporting policy and procedure suite that:

- **Incorporates all required processes for completion of the ITRM Framework including a robust challenge mechanism;**
- **Specifies the skill sets and training required of those responsible for completion of departmental components of the ITRM documents;**
- **Embeds the strengthened role of the CIO.**

Management Response

Management agrees with this recommendation.

Policies and procedures will be developed to incorporate the ITRM framework with appropriate challenge mechanisms. Requisite skills and training will be identified and included as part of the phasing in of the framework. This recommendation will be complete by Q4 2017.

Recommendation 7

That all City departments, with direction and support from ITS:

- **Ensure departmental staff preparing ITRM documents have the requisite skills and tools to adequately and completely prepare all required ITRM documents;**
- **Develop departmental processes which ensure that all components of the business line are included in required ITRM documents;**
- **Develop review and challenge mechanisms designed to ensure that all ITRM documents are completed to an appropriate level of granularity which fully**

facilitates the understanding of IT risks, impact and the management and tracking of strategies related to the mitigation of IT risks.

<u>**Management Response**</u>

Management agrees with this recommendation.

City management, with assistance from ITS, will include training, document preparation, risk escalation, challenge processes, tracking mechanisms and reporting as part of the enterprise wide roll-out of the ITRM framework. This recommendation will be complete by Q4 2017.

Recommendation 8

That the CIO as well as and City-wide managers continue to improve the identification and assessment of IT and related mitigation strategies, while using the ITRM Framework recommended in recommendations 1 and 2.

<u>**Management Response**</u>

Management agrees with this recommendation.

The principle of continuous improvement will be applied as the ITRM framework program is phased in to ensure continuous and improved identification and assessment of IT risk and related mitigation strategies. A senior oversight body, currently being established, will oversee the maturation of the ITRM framework. Once the ITRM framework is implemented, ITS will conduct assessments of new or emerging IT mitigation strategies on an annual basis.

Potential Savings

We believe the net impact of these recommendations will lead to overall efficiencies for the City in the following ways:

- Improved direction, advice and reporting of IT activities on a City-wide basis will lead to economies of scale and better decision making for IM/IT related decisions before they are made.
- Improved identification, assessment and mitigation initiatives will protect the City against potential system failures or security breaches, including cyber-attacks, which could interfere with business activities to the extent they could impact the life safety and daily lives of residents. The costs of repairing/restoring these activities could also be catastrophic. It could also undermine the public's confidence in the management of the City.
- Improved policies and procedures for minimizing waste could result in immediate savings to the city. For example, IT infrastructure loads and IT platform costs to support IM demand are always high, especially if IM demand (e.g. applications,

email management) is not rigorously controlled and monitored through policies, practices and awareness. Closer monitoring of the risk/cost of having more IT infrastructure than required could result in direct saving.

Notwithstanding these potential savings, it must be noted that necessary changes to upgrade/replace the City's infrastructure and to adequately increase the City's IT security protection will require significant investment in coming years.

Conclusion

Based on our review of the completed IT risk related documents and strategies, we have determined that there is a low maturity level of most City departments for IT Risk Management. This is primarily due to the Governance and Leadership issues identified in the key observations. The four ITRM Governance recommendations identified in the key observations will be required to be implemented prior to development of the remaining ITRM Framework recommendations (recommendations 5 through 8). Once the Governance component of the ITRM is completed, the remaining components will be much easier to efficiently develop and implement.

Without the recommended development of an ITRM Framework, including the roles, responsibilities and accountabilities, funding model and policy suite, the potential vulnerability of the IT risks could have significant impacts on the City's business lines. We highly recommend that the City develop the Management Action Plan for these recommendations, in consultation with the leading practises identified by ISACA in COBIT and the *RISK IT* Framework.

Acknowledgement

We wish to acknowledge our appreciation for the cooperation and assistance afforded the audit team by management.

The following section is the detailed audit report.

Detailed Audit Report

Introduction

The City of Ottawa's Audit Plan for 2014, as approved by Council in March 2014, included audits of Information Technology (IT) and related investments. This Audit of IT Risk Management, along with an Audit of IT Security Incident Handling and Response, were completed in accordance with the 2014 Audit Plan.

Background

Throughout the City, IT-based solutions and innovations have supported the achievement of a variety of operational and strategic objectives. The role of technology is expected to continue a steep growth pattern as new and innovative solutions are developed. However, while there are opportunities for IT to support the City's strategic objectives, there are a variety of traditional and emerging IT risks that must be considered and effectively managed at the highest level.

For an organization of the complexity and size of the City of Ottawa, the breadth and depth of potential IT-related risks is significant. Whether it's maintaining operational or administrative capabilities, protecting valuable or sensitive assets, supporting compliance or enabling achievement of business or strategic imperatives, there is an inherent risk relating to IT in nearly every City activity or function. As such, while there is obviously a technical element of IT risk, business managers from across the City are ultimately the most important stakeholders in the management of IT risks.

The City's Approach to IT Risk Management

The Enhanced Risk Management (ERM) Framework

In 2010, Council approved a conceptual Enhanced Risk Management (ERM) Framework and Enhanced Risk Management Policy. By 2011, the Framework had been implemented across the City. The Framework outlines roles and responsibilities for risk management, the City's risk management process, and provides other resources and tools for departmental managers and others with responsibilities under the Framework and Policy. Since 2011, City departments have annually conducted risk analysis activities which have led to the development of the Corporate Risk Profile (CRP).

IT Risk

IT risks are those associated with the use, ownership, operation, involvement, influence and adoption of IT within an organization. It consists of IT-related events that could impact the organization's ability to achieve its goals and objectives. Like most risks, they can occur with uncertain frequency and magnitude. Examples of IT risks include the loss/corruption of information assets, and the inability to provide IT-dependent business functions.

IT Risk Management Framework

The management of IT risks is supported through a number of policies, processes and practices at both an enterprise-wide and at a more granular level (e.g., at the IT project level or incident response level). At the enterprise level, IT-related risks are explicitly captured within the ERM Framework. While the Information Technology Services (ITS) Department is the single most significant source of IT risks, IT risks were identified by 65% of all departments in 2014.

The ITS Department plays an important role in the management of IT risks at the project and systems level. In addition to providing training/awareness sessions related to IT risks, ITS is responsible for developing IT related policies and guidance to support the management of IT risks. Some of the key policies developed to date include:

- Information Risk Management Policy (Jan 2012);
- Information Security Policy (Aug 2011);
- Information System Security Policy (Jun 2012);
- Remote Access to City Network Policy (May 2012); and the
- Responsible Computing Policy (Dec 2012).

ITS has a formal and broad responsibility for the management of IT risks, however, there are independent IT groups that serve in a few departments where one or more business applications or systems (e.g., SCADA[1] systems) that, while often connected to enterprise architecture, operate fully or in part, autonomously from ITS. These include Transit Services Department, Traffic Operation Branch, Drinking Water Services Branch and Wastewater Services Branch.

Audit Scope and Objectives

IT Risk Management and IT Security Incident Handling are both concerned with managing risks to information holdings and systems by making informed, risk-based decisions on security controls and practices. Both employ complementary controls and monitoring mechanisms, policies and standards. As such, the objectives and scope of this audit were designed to complement the OAG’s concurrent Audit of IT Security Incident Handling and Response.

[1] Supervisory Control and Data Acquisition (SCADA) refers to systems that are used to monitor and control industrial equipment, processes as well as buildings.

This audit focused on the design adequacy and effectiveness of IT Risk Management including the extent to which it aligned with the existing ERM Framework and supports a holistic approach to the management of IT risks across the City.

Audit Objectives

The overall objective of this audit was to provide an independent assessment relating to the adequacy and effectiveness of the City's IT Risk Management governance, policies, practices and procedures. Three (3) specific audit objectives were considered:

Objective No. 1: Assess if IT Risk Management Governance at the City effectively supports management of the City's IT-related risks.

Objective No. 2: Assess if the City's IT Risk Management Framework of policies, practices and procedures are adequately designed and aligned with the City's ERM Framework.

Objective No. 3: Assess if the City's IT Risk Management policies, practices and procedures are effectively supporting the identification, evaluation, mitigation and monitoring of IT risks across the City.

Audit Scope

The scope of this audit included IT risk management activities across the City of Ottawa. It involved an examination of both the design and effectiveness of controls (policies, practices and procedures). We reviewed roles, responsibilities and accountabilities as they exist both within ITS and across all City business lines and departments that use IT. This included an examination of IT risk management in areas where independent technology groups exist. Audit criteria (refer to **Appendix B**) were established to cover all areas of scope.

Audit criteria were established based on leading IT Risk Management guidance, specifically COBIT[2] and ISACA[3]. The ISACA *RISK IT* Framework, the most relevant and valuable source of leading practices, was used as a base for the development of audit criteria. Based on COBIT, this framework provides a comprehensive view of risks related to the use of IT and a thorough view of IT risk management, from the tone and culture at the top, to operational issues.

The scope of this audit did not involve assessments of:

[2] Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance.

[3] Information Systems Audit and Control Association (ISACA) provides globally recognized industry leading practices, guidance, benchmarks and other effective tools for all enterprises that use information systems.

- The appropriateness or application of technical IT controls related to security or other IT risks;
- The adequacy or effectiveness of the City's ERM Framework; or
- Those controls (technical and non-technical) related to the detection and response to IT security incidents.

Audit Approach

This audit was designed to ensure that sufficient and appropriate audit procedures were conducted and evidence gathered to provide reasonable assurance of the accuracy of audit findings and conclusions, as they existed at the time of the audit.

We assessed IT Risk Management policies, processes and practices for design adequacy and effective implementation both within ITS and across the City. The audit included an examination of the alignment of IT Risk Management with the City's Enhanced Risk Management Framework.

Document reviews, interviews and testing were performed during the audit fieldwork phase (April-June 2015).

Detailed Findings, Observations and Recommendations

Key Observations - Governance, Executive Leadership and Support

The City has a strong committee structure for addressing IT risk management. Following the Audit of IT Governance, tabled in March 2015, the reporting structure was strengthened, although this audit noted areas where improvement was required.

The City has experienced a high rate of turnover in the Director, ITS and Chief Information Officer (CIO) position over the past few years including extended periods where the position was occupied by a temporary replacement. A new Director, ITS and CIO was hired in the spring of 2015. We noted, that the ITS Staff interviewed as part of this audit were positive and enthusiastic regarding the new CIO's leadership, strategic direction and support.

Notwithstanding this positive development, the City has yet to develop a comprehensive Governance component of an Information Technology Risk Management (ITRM) Framework including clear and consistent responsibilities and accountabilities for City executives and management embedded in an ITRM Framework. In particular, the effectiveness of the existing ITRM Governance is impacted by several factors including:

a) Absence of an ITRM Framework with a comprehensive Governance component;
b) The method of prioritizing, selecting and funding IT initiatives;
c) Authority of Corporate Information Technology Management Team (CITMT); and
d) Authority of the CIO.

Each of these issues are discussed further below.

Governance Component to an ITRM Framework

While the City does have some components of an effective ITRM Framework embedded in the ERM, there is no stand-alone ITRM Framework with governance capable of supporting a mature risk culture. Effective governance within an ITRM would help to provide clear guidance on the City's IT risk appetite[4] and IT risk tolerance[5] as well as oversight on their application. Without clear direction and oversight on these key components, it is not possible to develop an effective ITRM Framework (refer to the next section, entitled "IT Risk Management Framework Design and Alignment" for additional discussion of ITRM Framework).

[4] Risk appetite – The broad-based amount of risk an enterprise is willing to accept in pursuit of its mission*

[5] Risk tolerance – The acceptable variation relative to the achievement of an objective (and often is best measured in the same units as those used to measure the related objective)*

* Committee of Sponsoring Organizations of the Treadway Commission (COSO) definitions

Prioritization and Funding of IT Projects

IT projects are brought forward for consideration by individual departments. Departments are required to identify each project's source of funding and are encouraged to only bring forward funded projects. Notwithstanding instances where unfunded projects have been identified and approved as priority investments, this approach means that approved projects may not always be aligned with corporate priorities.

There is little flexibility for required adjustments to the ITS infrastructure budget and/or other departmental budgets for high priority IT projects as a large portion of IT budgets are controlled by individual departments, not ITS. Some departments (Transit, Traffic, and Water) have large IT budgets and independent IT groups. These budgets are typically based on historical requirements which have then become part of their baseline budget. This scenario supports the continued investment in IT risk management within some departments while IT deficiencies and related risks in other business lines are not addressed.

In addition, there are a variety of funding mechanisms, often with specific constraints. For example, the water and sewer surcharge funding can only be used for very specific water and sewer related activities.

Therefore, there is a significant risk that high priority IT risks are not being adequately addressed on a timely basis if funding is not readily available to the business owner. This applies to ageing IT infrastructure owned by ITS as well as new and existing initiatives owned/managed by independent groups such as Water, Transit, Traffic and other Information Management/Information Technology which belongs to other departments.

Authority of CITMT

While the concept of the Corporate IT Management Team (CITMT) approval process is sound, the process is hindered by the process described earlier whereby projects submitted to CITMT for consideration in the annual corporate IT plan are typically only those which are already funded. Funding may be sourced from individual departmental budgets, external sources such as the Province of Ontario, or with "earmarked" funding. As such, the funding status of IT projects, rather than a City-wide and risk-based priority ranking system, is a significant factor in determining which projects are considered by CITMT for inclusion in the annual corporate IT plan.

This decentralized approach to funding IT projects and absence of a City-wide priority ranking system impacts the effectiveness of CITMT's authority relative to its mandate. Specifically its mandate is "to plan, provide oversight and strategic direction necessary to:

- Deliver an annual corporate IT plan with a clear connection to the Corporate Strategic Plans as approved by council and its boards;
- Represent individual departmental and corporate needs;
- Support ITS in delivering on its mandate to provide innovative and cost effective technology solutions to deliver maximum business value;
- Base decisions on corporate strategic plan."

CITMT terms of reference also state that "CITMT serves as the corporation's primary agent of technology direction, having been given the authority by the Executive Committee to exercise leadership when undertaking its roles". While not explicitly stated in the terms of reference, CITMT has an implicit responsibility for leadership in recommending a corporate IT plan that is reflective of risk-based IT priorities across the City. CITMT's authority to discharge this responsibility is hindered by the current IT project funding model as well as the City's existing capability to identify and prioritize City-wide IT risks as discussed later in this report. As a result, decisions made regarding IT investments/expenditures may not always be aligned with overall corporate priorities and/or risk management objectives.

Authority of CIO

The job description for the Director, ITS and CIO position (both roles are performed by the same position) states that, in addition to directing the operations of the ITS department, from a corporate perspective the CIO is to provide strategic leadership for planning and implementation of a broad range of business and enterprise IM/IT initiatives, to support the City's service delivery objectives.

The position is to play a major leadership role in organizing, managing, and strengthening a comprehensive IT/IM infrastructure that will support and transform the administrative and service delivery areas of the City, and support its mandate. As well, the position is to oversee the implementation of departmental strategies, conduct long range fiscal planning with respect to IT and IM and serve as senior advisor regarding IM/IT issues to Council, Committees of Council and Counsellors to disseminate strategic direction, advice and technical information. This is consistent with the *RISK IT* framework (see **Appendix C** for details).

However, the CIO's actual ability to influence and manage is limited as staff responsible for IT in various departments and agencies (e.g. Ottawa Public Health, Transit, Water, Wastewater, etc.) are not functionally accountable to the CIO and lines of authority are not always clear. Further, the audit team was not able to identify any clear and formal description, in the job description or otherwise, of the CIOs authorities or responsibilities regarding the City-wide IT risks.

The lack of clarity around the authority of the CIO impedes his ability to:

- Promote a culture that supports ITRM objectives including influencing change at an executive level and introducing IT change management throughout the City and influencing/managing City-wide spending related to IM/IT;
- Align City-wide IT funding with the highest priority City-wide IT strategic initiatives;
- Tackle the highest priority City-wide IT risks on a timely and strategic basis; and
- Ensure compliance with policies, procedures and enforce central reporting of ITRM activities.

The reporting structure to and from the CIO is not consistent with best practises. The *RISK IT* framework recommends that the CIO position be responsible for all City-wide processes including Risk Governance, Risk Evaluation and Risk Response (Refer to **Appendix D**) and that all subordinate IT management roles report to the CIO.

This would enable the CIO to both inform and advise the City Manager, who would have ultimate accountability for managing IT risk including funding of mitigation strategies and opportunities, as the CIO would control and answer for all IT related staff. It would also enable the CIO to better influence decisions to ensure that overall corporate priorities, such as maintaining the integrity of existing infrastructure and ensuring security receive the appropriate priority and related funding.

Ultimately however, to truly manage IT risk, and act on the opportunities which will transition the City of Ottawa into a leading “smart city, the CIO should have the authority, resources and ability to perform all the following:

- Manage Costs – Control the impact of IT spend on the enterprise;
- Keep the lights on – Ensure the IT and security needs are up and running;
- Act as an information broker - Provide insight to support business decisions;
- Generate ideas and solutions – Enhance business processes by being an active business partner;
- Deliver transformation – Prepare and develop the organization for change; and
- Bring business model innovation – Shape the future of the business with the right technology.

Recommendation 1

That the City Manager develop a robust Governance component of an ITRM Framework which:

- **Is aligned to the ERM Framework.**
- **Includes clearly defined roles, responsibilities, and authorities of City Executives and Management.**

- **Clearly establishes the basis for a corporate risk culture, including risk tolerance and risk appetite guidelines.**
- **Ensures that all mitigation strategies for risks identified as being above acceptable tolerance levels are considered for inclusion in the Annual Corporate IT Plan based on risk/priority, regardless of whether there is pre-approved funding identified.**

Management Response

Management agrees with this recommendation.

The City Manager will work with ITS and the Corporate Programs and Business Services department to develop a robust Governance component of an ITRM framework. Work done to implement this recommendation will be completed in conjunction with work being done to implement Recommendation 5. This recommendation will be complete by Q4 2016.

Recommendation 2

That the City Manager and City Treasurer undertake an assessment of IT spending to explore alternative funding models which will provide better alignment between mitigation of prioritized City-wide IT risks and funds available/provided and provide long term savings through improved, targeted IT spending.

Management Response

Management agrees with this recommendation.

The City Manager, CIO and City Treasurer will work to identify and implement a budgeting/funding model that will allow for the funding of risk items that are deemed unacceptable. This funding model will form a part of the ITRM framework referenced in Recommendation 5. This recommendation will be complete by Q2 2016.

Recommendation 3

That the City Manager take steps to strengthen the effective authority of CITMT including expanding reviews to include all City-wide IT risks and proposed/recommended mitigation strategies.

Management Response

Management agrees with this recommendation.

The City Manager, in conjunction with ITS will take steps to strengthen the effective authority of CITMT as part of the work being undertaken to implement

Recommendation 1. Processes will be developed to incorporate the role of a senior oversight body in the risk mitigation decision-making process. This work will be completed by Q4 2017.

Recommendation 4

That the City Manager take steps to strengthen and confirm the role, responsibility and accountability of the Director, ITS and CIO position including consideration of alignment with the best practices identified in the ISACA *RISK IT* Framework as well as functional reporting of all City departments and agencies to the CIO for all IT matters.

Management Response

Management agrees with this recommendation.

The City Manager will take steps to strengthen and confirm the role, responsibilities and accountabilities of the Director, IT and CIO. In addition, as part of work done to implement Recommendation 1, the City Manager will consider best practices as identified in the ISACA RISK IT Framework in determining appropriate functional reporting for IT matters. This recommendation will be complete by Q4 2016.

Key Observations - IT Risk Management Framework Design and Alignment

The City has yet to develop a comprehensive IT Risk Management (ITRM) Framework. While there are a variety of ITRM activities occurring (e.g. at the project and system level), as noted for Objective 1, the City has no clearly defined ITRM framework that serves to bridge the gap between ERM and more granular ITRM.

ERM processes are continuing to mature, including the relatively new and developing explicit classification of IT risk categories. Specifically, in 2015 the Technology Risks were changed from ten sub-categories, that were difficult to differentiate among, to six very different types of sub-categories – (1) Maintenance and Lifecycle, (2) Resource Unavailability, (3) Service Disruptions or Losses, (4) Social Media, (5) Software and Hardware renewal and (6) System failure. The new Technology risks provide much better alignment with types of IT risks than before and will provide clarity for grouping these risks moving forward.

However, while the City recently started identifying specific IT risks and embedding them in the ERM framework, there are many deficiencies in the documentation to support the identification, assessment and mitigation of IT risks. In particular, the design effectiveness of the existing ITRM framework is reduced by several factors including:

- Insufficient documented and approved ITRM framework with a supporting policy and procedures suite;
- Insufficient processes for the identification and assessment of City-wide IT risks;
- Weaknesses in challenge mechanisms for assessment of proposed/possible corrective measures;
- Insufficient training of ITS staff, IT professionals outside ITS and others who are non-IT professionals yet are tasked with performing IT risk assessment;
- Undocumented IT risk universe that would serve to support oversight and inform decision-makers; and
- Incompleteness of Business Technology Plan including how the plan is based on mitigating the highest risks/priorities as well as related timelines, costs and sources of financing.

Given the low maturity level of most City departments for ITRM and the broad and technical nature of IT risks, procedures and guidance at both the corporate and departmental level are not sufficient to ensure that the identification, evaluation, communication, mitigation, and monitoring of the most important IT risks is consistent, appropriate and timely. In addition, IT issues and priorities that are critical to City-wide objectives do not necessarily rise to the top.

These issues are discussed further below.

ITRM Framework – Responsibilities and Accountabilities

Responsibilities for those providing input to ITRM documents such as risk registers are not fully developed, beyond completion of the Corporate Risk Profile as part of the ERM process. We would have expected to find clear, and consistent responsibilities and accountabilities for all employees involved in the ITRM process, including a RACI (Responsible – Accountable – Consulted – Informed) type model, similar to the one in **Appendix D**, embedded in an ITRM Framework with a supporting policy suite and processes. As noted earlier in this report, leading practices developed by ISACA were used to assess the effectiveness of the City's ITRM. Specifically **Responsibility** (those who must ensure that the activities are completed successfully) and **Accountability** (those who own the required resources and have the authority to approve the execution and/or accept the outcome of an activity) within specific *RISK IT* processes (refer to **Appendix C**) were assessed. These deficiencies in the City's ITRM framework impact the City's ability to:

- Integrate the management of IT risk into the overall ERM, thus allowing risk-return-aware decisions;
- Ensure there is an effective challenge mechanism to support both completeness and accuracy of the risks identified and the assessments of impact;

- Make well-informed decisions about the extent of the risk, and the risk appetite and risk tolerance of the enterprise, and
- Understand how to respond to the risk.

Policies and Procedures

Existing corporate level policies and procedures, including the Information Risk Management Policy, are consistent with the ERM Framework, however there is limited guidance or formal controls for departments, including those with independent IT groups, on their authority or responsibilities when engaging in activities that may impact the City's IT risk profile. Existing policies focus primarily on security threats and breaches of confidentiality of information, such as the Responsible Computing Policy or the Technology Devices Policy. However, there is a lack of policy guidance around other IT-related risks such as use of cloud-based solutions or other 3rd party systems or services.

In addition, most departments:

- Have not developed their own policies, processes/procedures which reflect their unique IT risks, business objectives and environment; and,
- Rely on the annual ERM processes, ITS intervention, and/or potentially limited scope activities (e.g. Vulnerability Assessments - VAs) to address IT risk management.

Training and skill sets

The City conducts user training for IT systems and IM applications. However, while there is a large focus on security, there is a lack of training concerning the efficient use of IT resources.

In some business units, people who have little or no technical training are being tasked, under the ERM Framework, with the identification of risks and/or related mitigation strategies. As a result, there are gaps and weaknesses in the identification, assessment and mitigation of critical IT risks (security, confidentiality, integrity, availability, reputational, operational, compliance/legal, strategic, business continuity, etc.).

City-wide Business Technology Plan and ITS Strategic Plan

The 2011-2014 ITS Strategic Plan outlines how ITS will support the previous Term of Council Vision by providing information on strategic objectives and related ITS initiatives, and how they align with the City's strategic priorities. While it includes brief details of ITS' strategic initiatives including ownership, description and performance measures, it is limited in scope insofar as it presents a departmental view rather than a City-wide view of the City's IT strategy.

The Business Technology Plan (BTP), however does provide a City-wide view. The BTP provides a summary of planned activities including those related to ServiceOttawa, new projects, ongoing business initiatives and operational support. The audit team reviewed documentation (project charters, storyboards, risk assessments, change management strategies, and implementation plans, etc.) for three (3) IT projects in the BTP. While not all projects demonstrated a clearly documented linkage to corporate priorities, the most recently completed sample did include a clear reference to Council priorities and how the project would service to support these priorities. It will be important, going forward, that such linkages are consistently demonstrated.

IT Risk Universe

The process of identifying IT risks is first impeded by the absence of a full inventory of the IT universe across the City (applications, business owners, networks, interdependencies, etc.). In addition, there is no complete risk register (risks, impact, mitigation strategy, and status, etc.) that is developed with input from trained and qualified IT professionals.

This is a significant risk as there are several departmental IT groups which operate fully or in part independently from ITS (e.g. within Water, Wastewater, Transit, and Traffic). In addition to these independent IT groups, some departments operate applications which are not within the City's direct control (e.g. provincially mandated applications used by Ottawa Public Health). Further, there are a number of examples where business lines have acquired third party applications and/or leveraged cloud-based solutions for their business without ITS's involvement. Such applications inherently present IT risk to the City to the extent they are accessed via City computers, use City networks, and/or are otherwise connected to the City's IT infrastructure. This risk is potentially high, particularly where such applications contain personal and/or confidential information of the citizens of Ottawa.

In addition, there are legacy systems which continue to operate and rely on ageing IT infrastructure. These systems typically place considerable demand on resources responsible to support the ongoing operation and maintenance of these applications and related IT infrastructure.

Without a documented, complete and comprehensive inventory of all IT components and applications relying on the City's IT infrastructure, it is not possible to build a comprehensive risk register which identifies the IT risks, potential impact and required mitigation/corrective action.

Recommendation 5

That the CIO develop a robust ITRM Framework which:

- **Is aligned to the ERM Framework;**
- **Incorporates the recommended Governance component of an ITRM framework (Refer to recommendation #1);**
- **Includes clearly defined roles, responsibilities, and authorities for all City employees involved in ITRM;**
- **Incorporates a well-documented audit universe/inventory and a risk register;**
- **Incorporates a well-developed challenge mechanism conducted by trained and qualified IT professionals;**
- **Ensures that all mitigation strategies for risks identified as being above acceptable tolerance levels are communicated to Senior Management in a comprehensive and effective manner.**

Management Response

Management agrees with this recommendation.

The current ERM framework will be reviewed and the ITRM framework will be enhanced to include the policies, processes and authorities for the entire corporation. Risk tolerance guidelines will be developed to include the process whereby unacceptable risks will be escalated to the appropriate authorities. The annual budgeting exercise will include a risk mitigation component where unfunded risk reduction costs will be identified. This recommendation will be complete by Q4 2017.

Recommendation 6

That the CIO, in conjunction with the development of the ITRM Framework, develop a supporting policy and procedure suite that:

- **Incorporates all required processes for completion of the ITRM Framework including a robust challenge mechanism;**
- **Specifies the skill sets and training required of those responsible for completion of departmental components of the ITRM documents;**
- **Embeds the strengthened role of the CIO.**

Management Response

Management agrees with this recommendation.

Policies and procedures will be developed to incorporate the ITRM framework with appropriate challenge mechanisms. Requisite skills and training will be identified and included as part of the phasing in of the framework. This recommendation will be complete by Q4 2017.

Recommendation 7

That all City departments, with direction and support from ITS:

- **Ensure departmental staff preparing ITRM documents have the requisite skills and tools to adequately and completely prepare all required ITRM documents;**
- **Develop departmental processes which ensure that all components of the business line are included in required ITRM documents;**
- **Develop review and challenge mechanisms designed to ensure that all ITRM documents are completed to an appropriate level of granularity which fully facilitates the understanding of IT risks, impact and the management and tracking of strategies related to the mitigation of IT risks.**

Management Response

Management agrees with this recommendation.

City management, with assistance from ITS, will include training, document preparation, risk escalation, challenge processes, tracking mechanisms and reporting as part of the enterprise wide roll-out of the ITRM framework. This recommendation will be complete by Q4 2017.

Key Observations - IT Risk Management Approach Effectiveness

The issues related to governance and design noted earlier have significant implications on the effectiveness of ITRM across the City. While the ERM and Corporate Risk Profile processes and policies are followed and IT risks are routinely identified, evaluated and mitigated through the ERM or other activities, the following concerns exist regarding the completeness and quality of the final product:

- There is neither the culture nor capacity to support a complete and holistic view of IT risks and the effective management of these risks;
- Outputs may not have been subject to sufficient analysis, consideration and challenge by people with appropriate and sufficient skill sets/competencies to effectively perform this function;
- Some IT related issues may not be appropriately identified, assessed and subsequently escalated to both inform (awareness) and mitigate (plans and funding);
- It is not clear if all risks related to ageing infrastructure, data storage, network capabilities, etc. have been identified; and
- There is not always a linkage between the identification of a critical risk with the provision of sufficient resources allocated for effective mitigation.

For example, analysis of the IT category in the Corporate Risk Profile (CRP) revealed very little/no identification of some IT specific risks such as those raised in the Security Incident Handling report including out-sourcing, 3rd party software, cloud computing, oversight of IT vendors, disaster recovery/business continuity, software license management, end user computing, IT infrastructure loads and costs for IM demand.

Without a complete and comprehensive IT risk universe, there cannot be a common view of IT risks and the City cannot make risk-aware decisions. That is, the City cannot make decisions that consider the full range of opportunities and consequences from reliance on IT for success. As importantly, it is not possible for City staff to have a full understanding of all potential IT risks within the IT universe. That is, City staff, especially ITS, do not know what risks they are not aware of, and cannot anticipate what corrective measures are required.

Recommendation 8

That the CIO as well as and City-wide managers continue to improve the identification and assessment of IT and related mitigation strategies, while using the ITRM Framework recommended in recommendations 1 and 2.

Management Response

Management agrees with this recommendation.

The principle of continuous improvement will be applied as the ITRM framework program is phased in to ensure continuous and improved identification and assessment of IT risk and related mitigation strategies. A senior oversight body, currently being established, will oversee the maturation of the ITRM framework. Once the ITRM framework is implemented, ITS will conduct assessments of new or emerging IT mitigation strategies on an annual basis.

Potential Savings

We believe the net impact of these recommendations will lead to overall efficiencies for the City in the following ways:

- Improved direction, advice and reporting of IT activities on a City-wide basis will lead to economies of scale and better decision making for IM/IT related decisions before they are made.
- Improved identification, assessment and mitigation initiatives will protect the City against potential system failures or security breaches, including cyber-attacks, which could interfere with business activities to the extent they could impact the life safety and daily lives of residents. The costs of repairing/restoring these activities could also be catastrophic. It could also undermine the public's confidence in the management of the City.
- Improved policies and procedures for minimizing waste could result in immediate savings to the city. For example, IT infrastructure loads and IT platform costs to support IM demand are always high, especially if IM demand (e.g. applications,

email management) is not rigorously controlled and monitored through policies, practices and awareness. Closer monitoring of the risk/cost of having more IT infrastructure than required could result in direct saving.

Notwithstanding these potential savings, it must be noted that necessary changes to upgrade/replace the City's infrastructure and to adequately increase the City's IT security protection will require significant investment in coming years.

Conclusion

Based on our review of the completed IT risk related documents and strategies, we have determined that there is a low maturity level of most City departments for IT Risk Management. This is primarily due to the Governance and Leadership issues identified in the key observations. The four ITRM Governance recommendations identified in the key observations will be required to be implemented prior to development of the remaining ITRM Framework recommendations (recommendations 5 through 8). Once the Governance component of the ITRM is completed, the remaining components will be much easier to efficiently develop and implement.

Without the recommended development of an ITRM Framework, including the roles, responsibilities and accountabilities, funding model and policy suite, the potential vulnerability of the IT risks could have significant impacts on the City's business lines. We highly recommend that the City develop the Management Action Plan for these recommendations, in consultation with the leading practises identified by ISACA in COBIT and the *RISK IT* Framework.

Acknowledgement

We wish to acknowledge our appreciation for the cooperation and assistance afforded the audit team by management.

Appendix A – List of Acronyms

BTP	Business Technology Plan
CITMT	Corporate Information Technology Management Team
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRP	Corporate Risk Profile
DCM	Deputy City Manager
ERM	Enhanced Risk Management Framework
IM	Information Management
ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITRM	Information Technology Risk Management
ITS	Information Technology Services Department
OAG	Office of the Auditor General
RACI	Responsible – Accountable – Consulted – Informed
RRA	Roles, Responsibilities and Authorities
SCADA	Supervisory control and data acquisition
SMC	Senior Management Committee
VA	Vulnerability Assessment

Appendix B – Detailed Audit Criteria

Audit Objective 1

Assess if the City of Ottawa's governance structure supports effective management of IT-related risks.

1. Management has clearly defined and communicated roles, responsibilities, and accountabilities (RRA) for IT risk management and promote a culture that supports IT risk management objectives.
2. Senior level committees are in place and routinely receive and monitor information regarding management of IT Risks across the City including the effectiveness of risk management practices and the sufficiency of resources.
3. The City's appetite and tolerance of IT risks is defined, approved and communicated. Departments have formally accepted accountability for operating within tolerance levels for IT risks and for reporting exceptions.
4. There is a mechanism in place to support monitoring, escalation and follow-up of IT risk exceptions (e.g. risk exposures exceeding the City's appetite).

Audit Objective 2

Assess if the City of Ottawa has a formal, and effective approach to IT Risk Management, which is aligned with the City's ERM Framework.

1. Policies and guidance are in place to support effective, consistent and holistic management of the City's IT risks at both an enterprise and departmental level.
2. Enterprise level policies, processes and guidance are supported by Departmental (business line) policies, processes/procedures regarding the identification, evaluation, communication, mitigation, and monitoring of IT risks.
3. IT Risk Management procedures, policies, guidance, tools and techniques align with City's objectives and support planning, performance reporting and other decision-making.
4. IT Risk Management procedures, policies, guidance, tools and techniques are integrated, and consistent, with the City's ERM Framework.

Audit Objective 3

Assess if IT Risk management policies/ processes/procedures effectively support identification, evaluation, mitigation and monitoring of IT risks across the City.

1. IT-related risks, both inherent and residual, are routinely identified and evaluated across all departments as to their likelihood and impact.

2. IT-related risks that are evaluated as unacceptable are identified and appropriately communicated/escalated.
3. IT-related risk mitigation plans are appropriately approved and consider significance and duration for the risk exposure, and the probable costs and benefits of mitigation.
4. IT-related risk mitigation plans are routinely monitored for appropriate execution, identification of costs, benefits, and responsibility and approval of remedial actions (or acceptance of residual risks). Deviations from plans are appropriately communicated
5. IT risk findings are reported and rolled-up for the purpose of identifying and aggregating IT risk exposures and controls in support of a holistic view of IT risk across the City.

Appendix C: ISACA Risk IT Framework

To better understand the relevance of ISACA's *RISK IT* framework to the assessment of the City's ITRM Framework and why it was used for the assessment against best practices in conducting the audit, the following summary is provided.

ISACA's *RISK IT* framework identifies best practices and provides a framework for enterprises to identify, govern and manage IT risk. The *RISK IT* framework is based on the principles of Enterprise Risk Management, which have been applied to the domain of IT.

The *RISK IT* framework is about IT risk—business risk related to the use of IT. The connection to business is founded in the principles on which the framework is built, i.e., effective enterprise governance and management of IT risk, specifically:

- Always connect to business objectives;
- Align the management of IT-related business risk with overall ERM;
- Balance the costs and benefits of managing IT risk;
- Promote fair and open communication of IT risk;
- Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels; and
- Embed as a continuous process and part of daily activities.

RISK IT defines, and is founded on, a number of guiding principles for effective management of IT risk. The principles are based on commonly accepted ERM principles, which have been applied to the domain of IT. The *RISK IT* process model is designed and structured to enable enterprises to apply the principles in practice and to benchmark their performance.

The Risk IT Framework is comprised of three domains – Risk Governance, Risk Evaluation and Risk Response, each with three processes as follows:

1. **Risk Governance** – Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.

    - Integrate with ERM
    - Establish and Maintain a Common Risk View
    - Make Risk-aware Business Decisions

2. **Risk Evaluation** – Ensure that IT-related risks and opportunities are identified, analyzed and presented in business terms.

- Analyze Risk
- Maintain Risk Profile
- Collect Data

3. **Risk Response** – Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

   - Articulate Risk
   - Manage Risk
   - React to Events

Section 2.2 of the ISACA *RISK IT Framework* provides descriptions of each of the nine processes listed above.

Figure 1 below shows the interrelationships of the three domains (rectangles) and the nine related processes (circles) through a common linkage with Business Objectives and the two-way communication that must be in place to support such a framework.

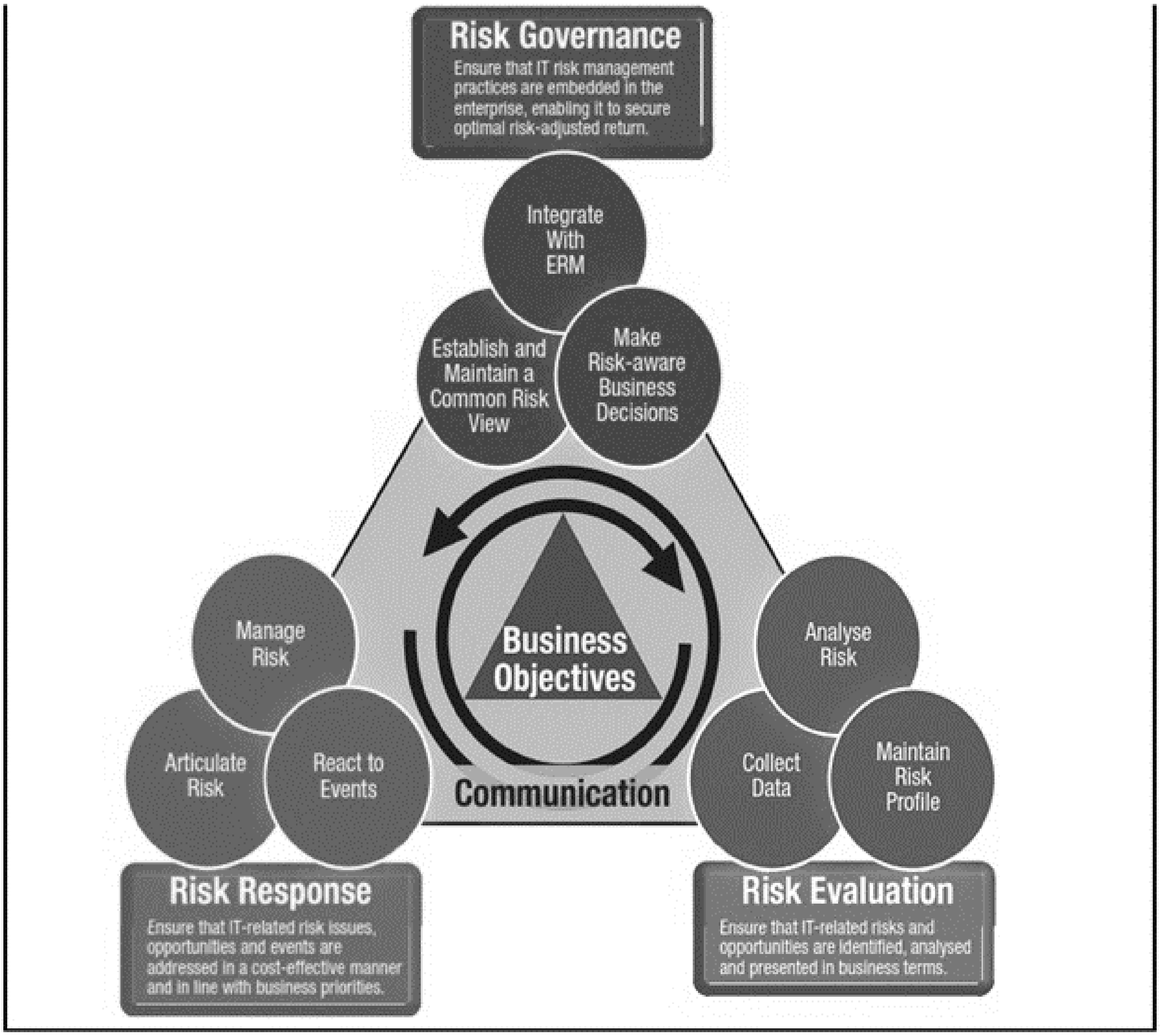
Risk Governance
Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.
Integrate With ERM
Establish and Maintain a Common Risk View
Make Risk-aware Business Decisions
Manage Risk
Articulate Risk
React to Events
Business Objectives
Communication
Analyse Risk
Collect Data
Maintain Risk Profile
Risk Response
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Risk Evaluation
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

Figure 1 – *RISK IT* Framework

Given that *RISK IT* framework is globally recognized for its leading practises in implementing IT governance and IT Risk Management (ITRM) and it is consistent with the City's ERM Framework, it was used as the benchmark against which to assess the City's IT Risk Management Framework.

Appendix D: ISACA RACI chart for IT Risk Management

The table below defines a number of roles for risk management and indicates where these roles carry responsibility or accountability for one or more activities within the 9 processes identified in Appendix C. The roles have been modified to align with positions in the City. The definitions are the ISACA definitions.

- **Responsibility** (R) belongs to those who must ensure that the activities are completed successfully,
- **Accountability** (A) applies to those who own the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific *RISK IT* processes. The *RISK IT* framework explains IT risk and enables users to make appropriate risk-aware decisions by:
- Integrating the management of IT risk into the overall ERM, thus allowing risk-return-aware decisions,
- Making well-informed decisions about the extent of the risk, and the risk appetite and risk tolerance of the enterprise, and
- Understanding how to respond to the risk.

Responsibilities and Accountability for IT Risk Management		**Risk Governance**			**Risk Evaluation**			**Risk Response**		
Role in IT RM Framework	**Definition for role in IT RM Framework**	**Common Risk View**	**Integrate with ERM**	**Risk-aware Decisions**	**Collect Data**	**Analyse Risk**	**Maintain Risk Profile**	**Articulate Risk**	**Manage Risk**	**React to Events**
Senior Management Committee	The most senior executives and/or non-executives of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources.	A	A							
City Manager (or CEO)	The highest-ranking officer who is in charge of the total management of the enterprise	R	R						A	
Chief risk officer (CRO)	The individual who oversees all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.	R	R	R	A	R	R	A	R	R
Chief information officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. The CIO typically chairs the governance council that manages the portfolio.	R	R	R	R	R	R	R	R	R
CFO	The most senior official of the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks	R								
Enterprise risk committee	The executives who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee.	R		R		R		R		
Business management	Business individuals with roles relating to managing a programme(s)	R	R	A		A	A	R	R	R

Responsibilities and Accountability for IT Risk Management		**Risk Governance**			**Risk Evaluation**			**Risk Response**		
Business process owner	The individual responsible for identifying process requirements, approving process design and managing process performance. In general, a business process owner must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities.	R	R	R	R	R	R	R	R	A
Risk control functions	The functions in the enterprise responsible for managing certain risk focus areas (e.g., chief information security officer, business continuity plan/disaster recovery, supply chain, project management office).	R	R	R	R	R	R	R	R	R
Human resources (HR)	The most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise.	R								
Compliance and audit	The function(s) in the enterprise responsible for compliance and audit.	R								R

Appendix E – List of Key Documents Reviewed

City of Ottawa Documents:

- Information Risk Management Policy
- Information Security Policy
- Information System Security Policy
- Remote Access to City Network Policy; and the
- Responsible Computing Policy
- Technology Devices Policy
- Employee Code of Conduct
- ERM Framework
- 2014 Business Technology Plan
- April 2014 Presentation “Secure Your Business – How a Risk Assessment Helps”
- 2014 Corporate Risk Profile
- 2014 Risk Inventory by Department
- Corporate Risk Practitioners Committee – December 2014 Agenda
- Director of ITS and CIO Job Description
- City of Ottawa Project Management Framework