The Corporation of the City of Windsor
Information Technology Governance

Final Internal Audit Report

8 January 2016

Distribution List

For action
Harry Turnbull, Executive Director of Information Technology
Matt Caplin, Deputy CIO /Manager of Project Management and Applications

For information
Helga Reidel, Chief Administrative Officer
Onorio Colucci, Chief Financial Officer
Stephen Cipkar, Executive Initiatives Coordinator

Limitations & Responsibilities

pwc

Contents

Summary of Internal Audit Results

The engagement has been performed in accordance with the scope of work per Appendix A.

Report Classification

In general, the City of Windsor ("CoW" or "City") has established and defined controls around Information Technology Governance to ensure the types and level of services provided to the City to meet its strategic and operational objectives in order to deliver the core services of the City, for example communications, human resources, and financial management. The City is aware of the importance of Information Technology Governance and the needs of the City with respect to the integration between the City's IT strategy and its business strategy. Additionally we noted that the City has established user groups for AMANDA and PeopleSoft, two important applications in the day-to-day operations of the city.

During the review of Information Technology Governance, we noted that the City is in the process of setting up an Enterprise Risk Management plan. This ERM plan will address an observation that was identified in the process for ongoing assessment of Information Technology Risks

IT Risk Management

The City has an established Project Management Methodology Policy that governs the execution of IT Projects based on their project scope, timeline, budget and risk. In addition, the Project Management Methodology Policy defines how Information Technology Risk and Information Security Risks are addressed as part of IT Projects.

While new IT Project Implementations are assessed for Information Technology Risks and Information Security Risks, it was noted that IT risk assessments are not currently being performed to identify and assess new IT Risks and Information Security Risks.

IT Process Framework

The City has an established IT Strategy for aligning IT resources to the City's strategic plan. The City also utilized the Ontario Municipal Benchmark Index which measures some of the City's IT services with other Municipalities.

It was noted that a documented IT Process Framework has not been implemented. The IT Process Framework should include IT processes, structures and relationships (e.g., to manage process gaps and overlaps), ownership, maturity, performance measurement, improvement, compliance, quality targets and plans to achieve them. The IT Process framework is an integration amongst the processes that are specific to IT, enterprise portfolio management, business processes and business change processes.

Based on the controls identified and tested as part of the Internal Audit of the City's Information Technology Governance, we have determined that there is reasonable evidence to indicate that:

	No or limited scope improvement	No Major Concerns Noted	Cause for Concern	Cause for Considerable Concern
Controls over the process are designed in such a manner that there is:				
Sample tests indicated that process controls were operating such that there is:				

Management has provided comprehensive action plans, which we believe will address the deficiencies noted.

Summary of Positive Themes

Overall, the City of Windsor has developed processes and controls around Information Technology and Governance.

IT Organization and IT Governance Structures: The City's IT Organization is organized and contains roles for IT functions including infrastructure, project management and other IT support services. The City has established a Technical Advisory Group ("TAG") that consists of senior members of the City and reports to City Council. Other City User Groups exist for AMANDA and the PeopleSoft applications.

Strategic and Operation Planning: The City has established a formal IT Strategy which defines the City's organizational dependencies related to IT.

Executive Leadership and Support: The City's Senior Leadership Team have set a clear vision for IT Support and Services that enables the City to achieve its IT Strategic Objectives.

IT Service Delivery and Measurement: IT has established Service Level Agreements with its users and IT services. The City is a member of the Ontario Municipal Benchmarking Initiative which measure some of the City's IT services with other municipalities in Ontario. OMBI results are presented to Council on a yearly basis for the City to measure the City's activities with other Ontario cities.

IT Organization and Risk Management: IT has an established Project Management Methodology framework to govern the execution of IT Projects appropriate for their scope, timelines, budget and risk.

IT Infrastructure and Enterprise Architecture: The City has formally established ownership responsibility for its key applications and supporting infrastructure.

Summary of Findings

Finding #	Topic	Rating[1]			Management Action
		Significant	Moderate	Low	
IT Organization and Risk Management					
1	Implementation of an IT Risk Management process to govern identification, assessment and communication of IT risk pertaining to information assets with the City's IT environment		X		Development of IT Security Risk Register – Technical Support Analyst – 2016 Q4
Service Delivery and Measurement					
2	Implementation of a formalized IT process framework with processes that are specific to IT, Business and business change process			X	Continue ongoing review of IT process and procedures – Manager of Project Management & Applications - Complete
Total			**1**	**1**	

Summary of Significant Findings

There were no significant findings noted during this audit.

Management Comments

It is important to note that this report has no significant findings. Similar to the findings in the October 2014 Manage Information Security Audit Report, and the June 2015 Manage Changes to Information Systems Audit Report, this is a good indication that the corporation is doing the right things to govern and manage its critical systems, infrastructure, data and resources.

This report has one "Moderate" finding and one "Low" finding. We are comfortable with these being noted as areas that could be improved upon.

Moderate finding: "*Implementation of an IT Risk Management process to govern identification, assessment and communication of IT risk pertaining to information assets with the City's IT environment.*"

- IT risk assessments are regularly carried out both formally (e.g. as part of the IT project process) and informally (e.g. assessing new threat information from vendors and other information sources). Security threats and vulnerabilities are regularly assessed, and plans and actions are determined based on those formal and informal assessments. We agree that the informal processes could benefit from the development of a more formal approach and documentation process.

Low finding: "*Implementation of a formalized IT process framework with processes that are specific to IT, Business and business change process.*"

- As noted in the Summary of Positive Themes above, the corporation has implemented a significant number of mechanisms to ensure the successful governance of its critical systems, infrastructure, data and resources, including policies, procedures and repeatable processes. We consider a "formalized IT process framework" a vision to guide the development of policies, procedures and processes, rather than a specific action item. E.g. In response to a finding in the June 2015 Manage Changes to Information Systems Audit Report, we used the ITIL framework (Information Technology Infrastructure Library) as a guide in developing four Change Management procedures. We are not aware of a municipality that would be considered to have "a completed formalized IT process framework", and PWC acknowledged that this finding usually stays active for a long period of time in most organizations. Over the years, we have made carefully considered decisions to use various best-practice components from various IT Frameworks in shaping the corporate IT environment. This is the preferred approach rather than a blanket commitment to implement a complete, end-to-end "formalized IT process framework", which we feel would result in significant upfront and ongoing costs that outweigh the benefits. We will continue to take this effective and cost-conscious approach, the benefits of which are evidenced in the findings of this audit, as well as the 2015 Manage Changes to Information Systems Audit , and the 2014 Manage Information Security Audit.

We are pleased with the thorough approach PWC used in conducting this audit and the previous audits. Both the process and the findings assist us in assessing opportunities for improvement.

Name: Matt Caplin
Title: Deputy CIO / Manager of Project Management and Applications
Date: 5/01/2016

Detailed Observations

Findings & Action Plans

<table>
<tr><th>Finding</th><th>Rating[1]</th><th>Recommendation & Action Plan</th></tr>
<tr><td colspan="3">1. IT Organization and Risk Management</td></tr>
<tr><td>Observation
Although IT risk assessments are carried out as part of new project implementation, it was noted that a continued IT risk assessment process to identify security threats, vulnerabilities and other safeguards based on asset's sensitivity is not being formally performed. Therefore project risks are assessed but no formal processes to assess and address ongoing and emerging operational risks for using information and technology in business was detected.</td><td rowspan="3">Overall
Moderate

Impact
Medium

Likelihood
Likely</td><td rowspan="3">Recommendation
Designing and implementing a process for identifying new risks and updating a risk register should be part of an ongoing risk management process with clear roles and responsibilities. A formal risk register should be developed and used. A risk register should include details of the types of risks, including description of risk, its category, cause, probability of occurring, and the impact on IT objectives, proposed responses/solutions, owners, and current status.

Management Action Plan

Expand upon the existing formal IT Security Framework and formal IT Security Methodology, to include a procedure and risk register to formalize the process for identifying and managing risks.

Responsibility
Steve Francia, Technical Support Analyst

Due Date
2016 Q4</td></tr>
<tr><td>Implication
Without a continued risk assessment process, risks might not be identified and addressed in a proactive manner resulting in the impairment of data integrity or breach of security, privacy or confidentiality.</td></tr>
<tr><td>Root Cause
Lack of ongoing Information Technology Risk Assessment process.</td></tr>
</table>

[1] See Appendix B for Basis of Finding Rating and Report Classification

Finding	Rating[2]	Recommendation & Action Plan
2. Lack of a formalized IT Process Framework		
Observation A formal IT process framework to execute the IT strategic/tactical plan containing process structure and relationships between processes that would address gaps and overlaps including ownership, performance measurement, improvement, compliance, and quality targets has not been formally established. The IT Process framework defines processes and controls and how they relate to operation and business needs. The IT Process Framework could be used to leverage good practices and provide service measures needs to recipients	**Overall** Low **Impact** Low **Likelihood** Likely	**Recommendation** Management should develop and implement an IT Process Framework. The IT Process Framework establishes the rules by ensuring adherence to the strategic plan and it integrates with processes that are specific to IT, Business processes and Business Change processes. **Management Action Plan** We will continue to develop and enhance corporate IT policies, procedures and processes based on selected best practices from various IT Process Frameworks in order to continuously improve the governance of the corporation's critical systems, infrastructure, data and resources. This is the incremental, continuous improvement approach that was started several years ago. It has no end date because there is always a need to improve and change policies, procedures and processes based on new risks, opportunities and priorities. We will continue to take this effective and cost-conscious approach, the benefits of which are evidenced in the findings of this audit, the Summary of Positive Themes noted above, the 2015 Manage Changes to Information Systems Audit findings, and the 2014 Manage Information Security Audit findings. A full implementation of a complete, end-to-end "formalized IT process framework", would result in significant upfront and ongoing costs that outweigh the benefits. We are comfortable with the ultimate objective of the Recommendation, and feel that the corporation's continuous improvement approach is the best fit for our organization, while working toward the same objective - ensuring meaningful and reliable IT processes and controls. **Responsibility** Matt Caplin, Deputy CIO/Manager of Project Management and Applications
Implication Lack of a formalized IT process framework increases the risk that process related to IT, Business process and Business change process are not clear.		
Root Cause Lack of a documented IT Process Framework.		

[2] See Appendix B for Basis of Finding Rating and Report Classification

		Due Date Complete

Appendix A: Background & Scope

Background

Linkage to the internal audit plan

As part of the 2015/16 Council approved Internal Audit Plan, Internal Audit will review processes surrounding the governance of information and technology at The Corporation of the City of Windsor (the "City") and the associated processes and controls to ensure that the governance framework is implemented.

As part of the internal audit plan development, this business process area has processes and controls associated with mitigating and managing the following corporate risks: Substandard Service Deliver, Implementation/Transition, Privacy/Security Breach, Service Failure and Technology Fails

Scope

As part of the internal audit plan development, the IT Governance for the City has processes and controls in place that govern the City's IT alignment with the City's corporate business strategy. IT Governance refers to the processes the City may be involved with in regards to supporting the business with applications and other related IT support. The City is using applications and systems including supporting infrastructure in processing and controlling a number of important business processes and operational activities. It is important that sufficient and appropriate IT Governance processes and controls would be in-place for these systems. The scope of our review includes those systems administered and managed by the City's IT Group and includes, but not limited to:

- ERP Applications;
- Desktop/laptop computers and peripherals;
- End user computing applications;
- Mobile devices and applications;
- Infrastructure: Networks and Hardware;
- Systems software, databases and operating systems; and
- Personnel and processes supported by IT.

The scope of this internal audit includes an assessment of IT Governance activities related to the most recent 12 month period (i.e. July 1, 2014 to June 30, 2015).

Overview of the business/process to be reviewed

As part of the internal audit of the governance of information technology at the City, internal audit will consider the processes and controls management has in place with respect to

1. Organization and governance structures:
    a. Govern information technology (structures, communication, and accountability) to provide the types and levels of service required by the City in order to achieve its strategic and operational objectives.
    b. Ensure the IT function understands the objectives and corresponding needs of the City and the degree of alignment and integration between City's IT strategy and its business strategy.
2. Strategic and operational planning:
    a. Develop and execute a strategic plan which defines organizational dependencies related to IT.

b. Document IT's role and responsibilities in achieving the objectives in the plan.
c. Develop, execute and monitor tactical operating plans which serve to support alignment of IT requirements and deliverables within the City's strategic goals.

3. Executive leadership and support:

a. Have City leadership set a clear vision for understanding and communicating how IT supports and enables the City to achieve its objectives.
b. Align IT investments with the City's strategy which will support the understanding of IT as a strategic enabler and not simply a cost. IT strategy, initiatives, projects and spending are aligned to City strategy and objectives.

4. Service delivery and measurement:

a. Ensure management processes and controls are sufficiently designed and operating to enable IT Planning, IT Delivery and Support, as well as Monitor and Evaluate.
b. Proactively manage IT spending including measurement of resulting value increases, such as greater Return on Investment (ROI), from IT investments. Sound IT governance also includes an effective performance management framework that captures the right quantitative and qualitative data to enable proactive measurement, analysis, and transparency.

5. IT Organization and Risk Management:

a. Ensure that the information and technical components of the IT environment are very well organized and clear direction is provided to IT through the City strategic plan and properly designed organizational structures.
b. Manage IT risks effectively in relation to meeting the City's needs and requirements.

6. IT Infrastructure and Enterprise Architecture:

a. Ensure the City's strategic policy on enterprise-wide architecture has been defined primarily on a formal assessment of business benefits in relation to meeting the City's needs and requirements.

Specific Scope Limitation

Consistent with commonly accepted practices the following are excluded from the scope of this review:

- The effective design, implementation and operation of the Information and Technology (IT) and general controls.
- The effective design, implementation and operation of business processes and application controls related to the capture, processing, storage, reporting/presentation and exporting of information and data.

Appendix B: Basis of Finding Rating and Report Classification

Findings Rating Matrix

Audit Findings Rating		Impact		
		Low	**Medium**	**High**
Likelihood	**Highly Likely**	Moderate	Significant	Significant
	Likely	Low	Moderate	Significant
	Unlikely	Low	Low	Moderate

Likelihood Consideration

Rating	Description
Highly Likely	• History of regular occurrence of the event. • The event is expected to occur in most circumstances.
Likely	• History of occasional occurrence of the event. • The event could occur at some time.
Unlikely	• History of no or seldom occurrence of the event. • The event may occur only in exceptional circumstances.

Impact Consideration

Rating	Basis	Description
HIGH	Dollar Value[3]	Financial impact likely to exceed $250,000 in terms of direct loss or opportunity cost.
	Judgemental Assessment	**Internal Control** Significant control weaknesses, which would lead to financial or fraud loss. **An issue that requires a significant amount of senior management/Board effort to manage such as:** • Failure to meet key strategic objectives/major impact on strategy and objectives. • Loss of ability to sustain ongoing operations: - Loss of key competitive advantage / opportunity - Loss of supply of key process inputs • A major reputational sensitivity e.g., Market share, earnings per share, credibility with stakeholders and brand name/reputation building. **Legal / Regulatory** Large scale action, major breach of legislation with very significant financial or reputational consequences.
MEDIUM	Dollar Value	Financial impact likely to be between $75,000 to $250,000 in terms of direct loss or opportunity cost.
	Judgemental Assessment	**Internal Control** Control weaknesses, which could result in potential loss resulting from inefficiencies, wastage, and cumbersome workflow procedures. **An issue that requires some amount of senior management/Board effort to manage such as**: • No material or moderate impact on strategy and objectives. • Disruption to normal operation with a limited effect on achievement of corporate strategy and objectives • Moderate reputational sensitivity. **Legal / Regulatory** Regulatory breach with material financial consequences including fines.
LOW	Dollar Value	Financial impact likely to be less than $75,000 in terms of direct loss or opportunity cost.
	Judgemental Assessment	**Internal Control** Control weaknesses, which could result in potential insignificant loss resulting from workflow and operational inefficiencies. **An issue that requires no or minimal amount of senior management/Board effort to manage such as:** • Minimal impact on strategy • Disruption to normal operations with no effect on achievement of corporate strategy and objectives • Minimal reputational sensitivity. **Legal / Regulatory** Regulatory breach with minimal consequences.

[3] Dollar value amounts are agreed with the client prior to execution of fieldwork.

Audit Report Classification

Report Classification	The internal audit identified one or more of the following:
Cause for considerable concern	• Significant control design improvements identified to ensure that risk of material loss is minimized and functional objectives are met. • An unacceptable number of controls (including a selection of both significant and minor) identified as not operating for which sufficient mitigating back-up controls could not be identified. • Material losses have occurred as a result of control environment deficiencies. • Instances of fraud or significant contravention of corporate policy detected. • No action taken on previous significant audit findings to resolve the item on a timely basis.
Cause for concern	• Control design improvements identified to ensure that risk of material loss is minimized and functional objectives are met. • A number of significant controls identified as not operating for which sufficient mitigating back-up controls could not be identified. • Losses have occurred as a result of control environment deficiencies. • Little action taken on previous significant audit findings to resolve the item on a timely basis.
No major concerns noted	• Control design improvements identified, however, the risk of loss is immaterial. • Isolated or "one-off" significant controls identified as not operating for which sufficient mitigating back-up controls could not be identified. • Numerous instances of minor controls not operating for which sufficient mitigating back-up controls could not be identified. • Some previous significant audit action items have not been resolved on a timely basis.
No or limited scope for improvement	• No control design improvements identified. • Only minor instances of controls identified as not operating which have mitigating back-up controls, or the risk of loss is immaterial. • All previous significant audit action items have been closed.