TORONTO

AUDITOR GENERAL'S REPORT
ACTION REQUIRED

Implementing an Integrated City-wide Risk Management Framework

Date:	June 11, 2015
To:	Audit Committee
From:	Auditor General
Wards:	All
Reference Number:	

SUMMARY

Every five years, the Auditor General's Office performs a detailed risk assessment of the operations of the City and those agencies and corporations included within its mandate. The purpose of the audit risk assessment is to identify high risk areas that will be prioritized for future audits. The exercise includes a high level evaluation of risks associated with the operations in City divisions, agencies and corporations.

During the Auditor General's assessment of risk across the City, it became apparent that while certain elements of an integrated enterprise-wide risk management (ERM) framework are present, a complete and formal framework is not in place.

Given the size and complexity of the City, a holistic approach to managing risk would be more appropriate. The application of an integrated enterprise-wide risk management framework is expected to enable management and staff to better understand the nature of risk, and to manage it more systematically.

This report includes one recommendation. Management's response to the recommendation is included as Attachment 1.

RECOMMENDATION

The Auditor General recommends that:

1. City Council request the City Manager review options for managing risks on an integrated basis across the City and report back to Council on a work plan and timeline for implementation. The review to consider:

a. an appropriate corporate Enterprise-wide Risk Management (ERM) policy and/or enterprise-wide framework for an integrated approach to managing risk across the City

b. the appropriate resources, tools, and job aids to be made available to divisions, agencies, and corporations, to support a common and consistent understanding of risk management processes and practices

c. the appropriate mechanisms for tracking and monitoring risks and to report on significant risks to City Council and/or appropriate committee of Council.

Financial Impact

Implementing the recommendation contained in this report will enable management and staff to better understand the nature of risk and to manage it more systematically. The implementation of an integrated ERM framework will require an investment of resources; however, the extent of expenditures that result from the implementation of the recommendation in this report is not determinable at this time.

DECISION HISTORY

The Auditor General's 2015 Audit Work Plan, adopted by City Council on March 31, 2015, included an audit of enterprise-wide integrated risk management practices. The purpose of the review was to perform a high-level assessment of how the City measures, prioritizes and manages its risks, and how this information filters up to the City Manager and ultimately City Council.

http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2015.AU1.8

ISSUE BACKGROUND

Every five years, the Auditor General's Office performs a detailed risk assessment of the operations of the City and those agencies and corporations included within its mandate. The purpose of the audit risk assessment was to identify high risk areas that will be prioritized for future audits. The exercise included a high level evaluation of risks associated with the operations in City divisions and agencies and corporations.

During the Auditor General's assessment of risk across the City, it became apparent that while certain elements of an ERM framework were present in some areas, a complete and formal integrated enterprise-wide risk management framework was not in place. A high level summary of the City's existing risk management activities is included in Appendix 1.

The Auditor General's Office has not completed an assessment of the quality, efficiency, and effectiveness of those components of an ERM framework that currently exist. The recommendation made in this report is based on the overall absence of an integrated approach across the City.

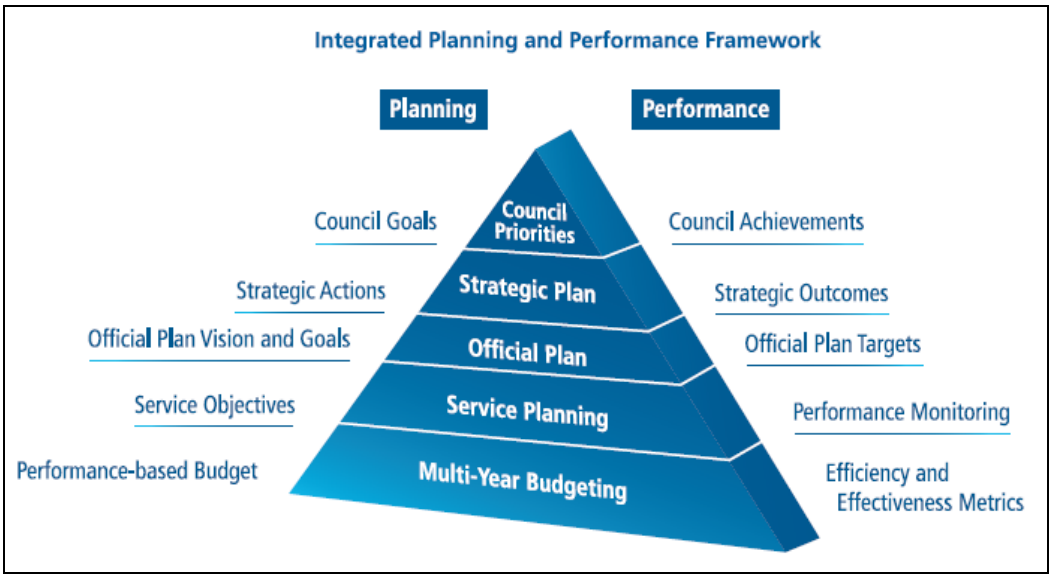
COMMENTS

In 2002, Toronto City Council approved its Strategic Plan. In 2012, the City Manager led the development of 26 new Strategic Actions for 2013 to 2018.

(http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2013.EX34.5)

The presentation to City Council indicated the City of Toronto employs an "Integrated Planning and Performance Framework" (as set out in the diagram below) that connects Council's goals to:

- Strategic Actions that are set to advance those goals
- The Official Plan, which guides growth and manages change with the objective of supporting city-building and enhancing quality of life
- Service planning that includes divisional business and sectoral plans
- Multi-year budgeting which sets the fiscal foundation and aligns these objectives.



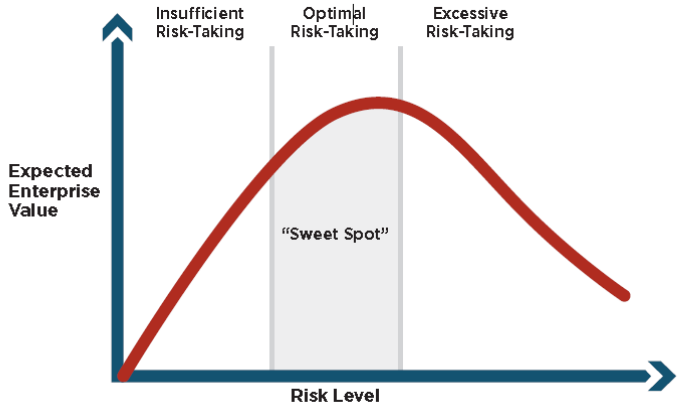
Source: http://www.toronto.ca/legdocs/mmis/2013/ex/bgrd/backgroundfile-61594.pdf

Risk management, not specifically contemplated in the Integrated Planning and Performance Framework, is a fundamental element of corporate governance. In general terms, integrated enterprise-wide risk management (ERM) is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.

A risk-free environment is nearly impossible. However, many risks can be reduced, mitigated, or eliminated. A common misperception is that the elimination of risk is the objective of an ERM system. A thought leadership paper, "Risk Assessment in Practice", sponsored by COSO noted:

> *"Given that risk is integral to the pursuit of value, strategic-minded enterprises do not strive to eliminate risk or even to minimize it, a perspective that represents a critical change from the traditional view of risk as something to avoid. Rather, these enterprises seek to manage risk exposures across all parts of their organizations so that, at any given time, they incur just enough of the right kinds of risk—no more, no less—to effectively pursue strategic goals. This is the "sweet spot," or optimal risk-taking zone, referred to in exhibit 1."*

Exhibit 1: Optimal Risk-Taking



Source: http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf

Optimal risk-taking also supports the development of effective and efficient controls by recognizing the point of diminishing returns when the cost outweighs the benefit, as well as where complexity of risk avoidance can actually increase risk.

ERM systems require the prioritization of risk in order for management to focus and thus more effectively manage the most important opportunities and threats. Good risk management results in managing negative risks and in leveraging opportunities to ensure value for money is achieved.

Canada's former Auditor General, Sheila Fraser, identified in 2003 the importance of integrated risk management frameworks in the public sector. Integrated risk management helps to "*take the guesswork out of managing risk*" and goes "*a long way toward creating a risk-smart work force and a culture in the public service that promotes innovation, while at the same time protecting the public interest and maintaining public confidence.*" Integrated risk management is "*not only vital to managing resources more efficiently and making better decisions, but ultimately it will contribute to making the public service more effective*".

The former Auditor General for Canada further noted that "*a sound and systematic approach to risk management distinguishes managing effectively from merely coping.*"

A risk management framework with a common classification, consistent methodology, and/or tools for use across the City has not been established. As a result, there is a lack of common understanding of risks across the entire organization. For example, "risk management" is often only referred to in the context of exposures addressed through insurance. Similarly, "risk assessment" is often thought of in the context of fraud risks or risks to financial reporting or financial control. Seldom are divisions conducting formal risk assessments that contemplate broader strategic or governance risks, reputation risks, and/or human risks (social responsibility). A glossary of risk-related terminology is included in Appendix 2.

Risk management is delegated to individual divisions to address

Although the City does not have an integrated ERM framework, the City has assigned certain types of risk to individual divisions or units to deal with.

During the Auditor General's 2014 City-wide risk assessment, 16 out of 58 City divisions, agencies, and corporations indicated they had formal risk assessment processes in place. Information provided by the division, agency, or corporation indicated that these processes were specific to its operations, services, and/or activities and the scope of the risk assessments were generally limited to one or more of the following types of risks:

- Compliance risks identified based on legislated requirements and/or provincially defined standards
- Operational risks
- Fraud risks
- Project specific risks

In addition, certain City divisions were delegated responsibility for managing specific forms of risk for the Corporation as a whole and have implemented forms of risk assessment to address those specific risks. Risk assessments at the corporate level include:

- Major issues with the City's financial position which can impact the achievement of the City's long term financial plan
- Exposures to accidental losses considered as part of the City's property and casualty insurance program
- Hazard identification as part of the City's Emergency Management Plan
- Threat assessments related to the City's Corporate Security Plan
- Threat and vulnerability assessments of the City's Information & Technology infrastructure

In addition, as part of the annual budgeting process, program / service specific key challenges and priority actions were described in the Analyst Notes for City Council's attention.

The corporate and departmental risk assessments, summarized above and further described in Appendix 3, were conducted for varying purposes using vastly different approaches. There was no common scale for impact and likelihood against which identified risks were analyzed, evaluated, and prioritized. As a result, the output of these processes also varied significantly, and in some cases a documented and up-to-date risk register has not been produced.

The various risk management activities across the City do not provide a comprehensive enterprise-wide view of risk

Given the financial constraints facing the City as a whole, an enterprise-wide view of risks should be readily available when contemplating the competing objectives and priorities of the individual divisions, agencies, and corporations as well as the City as a whole.

The City does not have formal communications and reporting mechanisms for keeping stakeholders continuously informed of organizational risk management processes, practices, and risk responses.

Key risks, both internal and external, that could significantly influence overall City priorities, performance, and achievement of corporate objectives, as well as their likelihood and their potential impacts should be available "at a glance". Risks at the operational level should be aggregated, if applicable, and then prioritized to create a succinct list of the organization's key risks that require executive management and City Council attention.

The City is lagging behind in its approach to risk management when compared to other public and private sector organizations

Other Canadian municipalities much smaller in size and budget than the City of Toronto have adopted ERM, integrated risk management, or other similar frameworks including:

- City of Burlington
- City of Calgary
- City of Edmonton
- City of Guelph
- Regional Municipality of Halifax
- City of Ottawa
- City of Vancouver
- City of Windsor

In addition, various provincial governments including the Provinces of Alberta, Ontario, British Columbia, and the federal government have implemented ERM frameworks.

An ERM policy and framework should be defined

A corporate ERM policy and framework should reinforce to all City employees their responsibilities related to risk management and create awareness of the process to identify risks and what must occur once potential risks are identified.

The policy should emphasize that the management of risks should be integrated into the day-to-day operations and administration of the City. The policy should address:

- the objectives and rationale for managing risk
- the linkage between risk management and the City strategic plan objectives as well as the strategic / business / service plan objectives of its divisions, agencies, and corporations
- the extent or range of risks that need to be managed
- guidance on what may be regarded as an acceptable level of risk
- the level of documentation required
- persons responsible for managing risk
- the centralized supports / expertise available (i.e., corporate ERM function), if any, to assist those responsible for managing risk
- plans for audit, review and/or evaluation of the City's (divisions, agencies, and corporations) performance in regard to the management of risk.

However, a corporate ERM policy will be effective only if staff are provided the appropriate tools and job aids to support a common and consistent understanding of risk management processes and practices. A summary of potential resources to aid the City in implementing an ERM framework is included in Appendix 4.

From an efficiency perspective, the City should centrally develop the framework, toolkit, and any other necessary resources to support the implementation of ERM. These should be shared with the City's agencies and corporations.

Where existing projects are currently underway within City divisions or agencies and corporations, the City should consider leveraging such projects, where possible. For example,

- The City's Human and Social Services cluster of divisions (Cluster A) is planning to complete an ERM project by January 2016 using a consistent approach across the Cluster to identify and assess risks and set out plans for identified risks. This project is currently limited to operational risks of divisional programs, services, and activities and does not address high level strategic risks.

- A City-Wide Business Continuity Management (BCM) Program is currently being developed. The purpose of the BCM Program is to develop, implement and maintain a business continuity program for all Divisions that enables each Division's effective response and recovery, in an orderly manner, to unplanned interruptions that disrupt critical services and operational functions while:

    - Ensuring the safety of the public and employees
    - Ensuring and maintaining the confidence and reputation of government
    - Minimizing potential revenue loss
    - Reducing the probability of disaster or disruption occurrence
    - Reducing the impact related to a disruption of services/operations
    - Protecting the critical infrastructure of the City of Toronto
    - Meeting regulatory requirements

    The BCM program is intended to formalize and to provide guidelines for developing, maintaining and exercising Business Continuity Plans for all Divisions.

- The Toronto Transit Commission (TTC) plans to implement an ERM program by 2017 which will:

    - Integrate risk management into the TTC`s culture and business processes
    - Achieve a balance between risk reduction and the cost of risk control
    - Monitor and diligently maintain the integrity and effectiveness of risk controls
    - Communicate and provide visibility to risk
    - Inform strategic decision making including the prioritization of capital

- Other City agencies and corporations including Toronto Community Housing Corporation have plans to establish ERM but such programs have not progressed significantly.

There are a number of existing software applications in the marketplace that have been developed to facilitate enterprise risk management, risk assessment, and/or risk reporting. To our knowledge, only the TTC has acquired a software platform to facilitate monitoring, communication, and reporting of their ERM program.

Conclusion

A successful ERM initiative is an ongoing process to strengthen risk management practices. Consideration and development of an ERM framework and toolkit, as well as comprehensive event identification, risk assessments, and risk responses cannot be achieved instantaneously. Instead, options for managing risks on an integrated basis across the City should be reviewed, and short and long term plans should be established to implement a framework in stages leveraging work that has already been completed in many divisions.

Short-term plans should focus on enterprise-wide risks and significant risks to achieving departmental objectives. Longer-term plans should focus on enhancing operational risk assessment processes over time and on a continuous or iterative basis. If action on the recommendation is to occur in a timely manner, then dedicated resources must be assigned to oversee and implement the action required. Appointing a project manager to develop an implementation plan and oversee the implementation, as well as the assignment of specific resources to deal with information technology and other requirements, is strongly recommended.

CONTACT

Jerry Shaubel, Director, Auditor General's Office
Tel: 416-392-8462, Fax: 416-392-3754, E-mail: jshaubel@toronto.ca

Ina Chan, Senior Audit Manager, Auditor General's Office
Tel: 416-392-8472, Fax: 416-392-3754, E-mail: ichan3@toronto.ca

SIGNATURE

_____

Beverly Romeo-Beehler, Auditor General

ATTACHMENTS

Attachment 1: Management's Response to the Auditor General's Report, "Implementing an Integrated City-wide Risk Management Framework"

Appendix 1: Summary of the City's Existing Risk Management Activities Against the COSO "Enterprise Risk Management - Integrated Framework"

Appendix 2: Glossary of Common Risk Related Terminology

Appendix 3: Examples of Existing Departmental and Corporate-Level Risk Assessments

Appendix 4: Resources to Aid in the Adoption of an ERM Framework

ATTACHMENT 1

Management's Response to the Auditor General's Report
"Implementing an Integrated City-wide Risk Management Framework"

Rec. No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
1.	City Council request the City Manager review options for managing risks on an integrated basis across the City and report back to Council on a work plan and timeline for implementation. The review to consider: a. an appropriate corporate Enterprise-wide Risk Management (ERM) policy and/or enterprise-wide framework for an integrated approach to managing risk across the City b. the appropriate resources, tools, and job aids to be made available to divisions, agencies, and corporations, to support a common and consistent understanding of risk management processes and practices c. the appropriate mechanisms for tracking and monitoring risks and to report on significant risks to City Council and/or appropriate committee of Council.	X		To ensure proper due diligence, there is a need to fully understand the cost and effort involved in implementing a risk management framework. The City has a number of risk management practices already in place across the City, both corporately and at the divisional level which forms a strong foundation upon which we can develop an effective risk management program. To ensure a value added approach these risk mitigation practices strive to balance the cost of controls with maintaining efficient and effective operations and service delivery.	The City Manager will perform a comprehensive investigation before making recommendations to ensure the selection of the best approach for integrated risk management. It will include the following step: • Discussion with similar organizations like Ottawa to further understand their approach, and actual costs and benefits of an ERM system. • Review of ongoing City initiatives to implement ERM within divisions. • Research on different types of modules that are available for integrated risk management. • Investigation of various types of risk tracked throughout the City and analysis on the feasibility of various frameworks. • Preliminary cost estimates for implementing an integrated system throughout the City. • Literature reviews that focus on the organizations that have implemented a form of ERM and their realized benefits and challenges. Report to Council – Q2, 2016

APPENDIX 1

Summary of the City's Existing Risk Management Activities Against the COSO "Enterprise Risk Management - Integrated Framework"

One prominent source for guidance on risk management is the "Enterprise Risk Management - Integrated Framework" of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This Commission, a private sector initiative, was formed in 1985 and in 2004, following some high profile corporate scandals, issued a framework to assist corporate management in evaluating and improving their risk management.

http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

The "ERM at a Glance" table below provides a high level summary of the City's existing risk management activities against the COSO framework. A glossary of risk-related terminology is included in Appendix 2.

ERM AT A GLANCE			
Enterprise Risk Management consists of eight interrelated components:	***Results***		
	Exists	*Partially exists*	*Does not exist*
A) Internal Environment – The internal environment encompasses the tone of the organization, influencing the risk consciousness of its people, and is the baseline for all other components of ERM. Expected internal environment factors include: • The City's Risk Management Philosophy • The City's Risk Appetite • Oversight by City Council • The integrity, ethical values, and competence of the City's people • The way management assigns authority and responsibility, and organizes and develops its people.		*The City's Risk Management Philosophy and Risk Appetite are not formally defined at the corporate level.* *Risk appetite has been defined for some but not all divisions, agencies, and corporations, albeit in an inconsistent manner.*	

	Results		
	Exists	*Partially exists*	*Does not exist*
B) Objective Setting – Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. Establishment of objectives is a precondition to effective Event Identification, Risk Assessment, and Risk Response.	√		
C) Event Identification – Management identifies potential events that, if they occur, will affect the City, and determines whether they represent opportunities or whether they might adversely affect the City's ability to successfully implement strategy and achieve objectives. Potential events are captured in an Event Inventory or Risk Register.		*In the absence of comprehensive Event Inventories or Risk Registers at the corporate and departmental levels, we are unable to assess the completeness and adequacy of event identification.*	
D) Risk Assessment – The City considers the extent to which potential events have an impact on achievement of objectives. Risks are analyzed from two perspectives, likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.		*Some forms of risk are identified and assessed on a departmental and/or enterprise-wide basis.* *Responses to identified risks exist within some but not all divisions, agencies, and corporations.* *The risk assessments together with risk responses may or may not be kept up to date.*	
E) Risk Response – Having assessed relevant risks, management determines how it will respond. Responses include risk avoidance, reduction, sharing, and acceptance.			
F) Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out. Control activities occur throughout the organization, at all levels and in all functions.	√		

	Results		
	Exists	*Partially exists*	*Does not exist*
G) Information and Communication – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity. There is effective communication with City Council and Boards of Directors of agencies and corporations.		*Some risk information is communicated; however, the City does not have formal mechanisms for identifying, capturing, and communicating appropriate risk related information down, across, and up the organization.*	
H) Monitoring – Enterprise risk management is monitored – assessing the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate audits or evaluations, or a combination of the two. Enterprise risk management deficiencies are reported upstream, with serious matters reported to Executive Management and City Council.		*Certain risk management activities are monitored; however, a corporate process for monitoring risk management activities is not in place.*	

APPENDIX 2

Glossary of Common Risk Related Terminology

The definitions presented in this glossary are consistent with those in COSO's "Enterprise Risk Management - Integrated Framework".

http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

Other frameworks including ISO 31000 – Risk Management may have slight variations in the definitions of these terms.

http://www.iso.org/iso/home/standards/iso31000.htm

Enterprise Risk Management	A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
Event	An incident or occurrence, from sources internal or external to an entity, that affects achievement of objectives. Potential events with positive impact represent opportunities, while those with negative impact represent risks.
Impact	Result or effect of an event. There may be a range of possible impacts associated with an event. The impact of an event can be positive or negative relative to the entity's related objective. *Some entities define impact scales for opportunities as well as risks. Impact assessment criteria may include financial, reputational, regulatory, health, safety, security, environmental, employee, customer, and operational impacts.*
Likelihood	The possibility that a given event will occur. Terms sometimes take on more specific connotations, with "likelihood" indicating the possibility that a given event will occur in qualitative terms such as high, medium, and low, or other judgmental scales, and "probability" indicating a quantitative measure such as a percentage, frequency of occurrence, or other numerical metric.

Opportunity	The possibility that an event will occur and positively affect the achievement of objectives.
Risk	The possibility that an event will occur and adversely affect the achievement of objectives. Inherent Risk – The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual Risk – The remaining risk after management has taken action to alter the risk's likelihood or impact.
Risk Appetite	The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (or vision).
Risk Assessment	Risks are analyzed, considering the likelihood that a given risk will occur and its potential impact, as a basis for determining how they should be managed. In assessing risk, management considers expected and unexpected events. Risks are assessed on an inherent and a residual basis. *The COSO Enterprise Risk Management – Integrated Framework calls attention to interrelated risks, describing how a single event may create multiple risks. Enterprise risk management encompasses the need for management to develop an integrated enterprise-wide view. With managers responsible for business unit, function, process, or other activities having developed a composite assessment of risk for individual units, entity-level management considers risk from an integrated enterprise-wide perspective.*
Risk Management Philosophy	An entity's risk management philosophy is the set of shared beliefs characterizing how the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities. Its risk management philosophy reflects the entity's values, influencing its culture and operating style, and affects how enterprise risk management components are applied, including how risks are identified, the kinds of risks accepted, and how they are managed.
Risk Register (or Event Inventory)	Inventory of potential events (risks or opportunities). The event inventory or risk register often contains all information related to potential events.

Risk Response As part of enterprise risk management, management considers potential responses with the intent of achieving a residual risk level aligned with the entity's risk tolerances.

Risk responses fall within the following categories:

- Avoidance – Exiting the activities giving rise to risk.
- Reduction – Action is taken to reduce likelihood or impact, or both.
- Sharing – Reducing risk likelihood or impact by transferring or otherwise sharing a portion of risk. Common techniques include purchasing insurance products, engaging in hedging transactions, or outsourcing an activity.
- Acceptance – No action is taken to affect risk likelihood or impact.

Risk Tolerance The acceptable variation relative to achievement of an objective.

APPENDIX 3

Examples of Existing Departmental and Corporate-Level Risk Assessments

During the Auditor General's 2014 City-wide risk assessment, 16 out of 58 City divisions, agencies, and corporations indicated they had formal risk assessment processes in place. Information provided by the division, agency, or corporation indicated that these processes were specific to its operations, services, and/or activities and the scope of the risk assessments were generally limited to one or more of the following types of risks:

- Compliance Risk Assessments – Certain divisions are required to conduct risk assessment to comply with provincial legislation and/or standards. For example,

    - Toronto Water conducts a risk assessment every 36 months as required by the Ministry of the Environment and Climate Change's Drinking Water Quality Management Standard. The risk assessment focuses on the critical points at which control can be applied to prevent, eliminate, or reduce drinking-water health hazards.

    - Toronto Paramedic Services is subject to Ministry of Health and Long-Term Care certification reviews of its Ambulance Services and of the Central Ambulance Communications Centre for compliance with related standards and legislation.

- Operational Risk Assessments – Certain divisions have attempted to review their operational risks albeit with vastly different approaches. For example,

    - Toronto Long-Term Care Homes and Services has adopted a Risk Management Framework policy to assure optimal care, service, and safety for residents / clients and to reduce and/or eliminate potential risks, actual risks, and the residual effects of risk. The Division has also implemented an Integrated Quality Management Framework policy to consider and act on opportunities to improve in areas related to strategic direction, quality improvement, risk management, safety culture, resource allocation (including positive work life culture) and ethics culture.

    - The Toronto Zoo has implemented various risk management and loss prevention systems to address risks to staff and contractor related systems, property related systems, public related systems, and animal related systems.

    - The Parks, Forestry, and Recreation division has identified risk areas and mitigation strategies including diversity and discrimination risk, employee relations risk, performance and responsibility risk, safe environment risk, client / customer risk, efficiency risk, privacy and confidentiality risk, project management risk, fraud and theft, process risks, unauthorized

activity risk, vendor performance risk, technology risk, property and third party liability risk, and financial risk.

- The Solid Waste Management division completed a baseline review of all business units across its four Sections in 2014. This review included a "risk ranking" of key activities within each unit as they relate to quality (best practices), health and safety compliance, and environmental compliance. However, the review does not appear to identify associated risk management strategies for the risk-ranked activities.

The outputs of these operational risk assessments varied greatly but, in general, comprehensive risk registers were not produced. Therefore, we were unable to assess the completeness and adequacy of event identification, risk assessment and related risk responses.

- Fraud Risk Assessment and Fraud Action Plans – City divisions have fraud action plans to address fraud and abuse within the division. In 2013, the City's Internal Audit Division assessed the effectiveness of certain divisional fraud action plans and concluded that the existing plans did not outline all fraud risks associated with the divisions and effective controls to mitigate fraud risks. Internal Audit made recommendations to improve mitigation of fraud and will follow up on the status of implementation of these recommendation during 2015.

- Project Risk Assessments – Certain divisions identified that they conduct risk assessments to identify and manage risks on specific projects.

The City has also developed processes to address some specific forms of risk that impact the corporation as a whole. For example,

- The Deputy City Manager and Chief Financial Officer reports on the City's financial condition and performance as part of the City's Annual Financial Report. The report includes a scorecard of the current status of the major financial issues relating to expenditures, revenues, and assets and liabilities identified in the City's 2005 Long-Term Financial Plan. The report summarizes key risks the City continues to face that could have a negative impact on the City's financial future and actions taken / to be taken to help address them. These risks include: lack of long-term dedicated funding to assist the City in addressing its infrastructure deficit, including building and expanding the transit system to meet the City's strategic goals, and accessing non-property tax revenue sources that grow with the economy to ensure long term sustainable funding.

- The Insurance and Risk Management section within the Corporate Finance division is responsible for the City's property and casualty insurance program. The Section has responsibility for cost effectively managing the City of Toronto's exposures to accidental losses (from personal injury or property damage) in ways which protect the City's assets and assure continuity of its operations.

- The Office of Emergency Management (OEM) has identified and assessed the various hazards and risks to public safety that could give rise to emergencies and has identified the facilities and other elements of the infrastructure that are at risk of being affected by emergencies. The City's Hazard Identification and Risk Assessment include 33 hazards of concern grouped into three broad categories: Natural Hazards, Human-caused Hazards, and Technological Hazards. The OEM leads and facilitates all City activities related to the City's ability to mitigate, prepare for, respond to, and recover from major emergencies. The City of Toronto Emergency Plan unifies the efforts of City and its agencies and corporations for a comprehensive approach for responding to and reducing the impacts of a public emergency. Risk-specific plans are developed to support the Emergency Plan which contain specific response plans for hazards that may pose a threat to the City of Toronto.

- In consultation with each City division, the Corporate Security division develops a Divisional Security Plan that documents current security measures in place and identifies gaps that should be addressed. Each plan includes a risk assessment based on methodologies set out in the "Harmonized Threat and Risk Assessment Methodology" from the Federal Communications Security Establishment and the "General Security Risk Assessment Guideline" from ASIS International. Once the assessment is completed Corporate Security proposes an action plan for the division to implement the recommendations. Such plans are generally reviewed and updated annually.

- Information Technology Threat and Vulnerability Assessments – The Technology Infrastructure Services Unit is responsible for developing processes and controls to meet City's information security needs. The Unit performs threat risk assessments, vulnerability assessments and when required a privacy impact assessments. The Information and Technology Division has also implemented solutions for intrusion detection and detection of security breaches through monitoring applications. The Risk Management and Information Security Group within the Division investigate incidents of security breaches and fraud related matters. Although the Division does not have a comprehensive document on City wide technology risks and controls, the Division has developed documentation for various policies and procedures and risk assessment for individual applications to deal with specific threats.

APPENDIX 4

Resources to Aid in the Adoption of an ERM Framework

AICPA

The AICPA (American Institute of Certified Public Accountants) has numerous resources to help members learn more about ERM and share with their senior management and staff, including:

- "2015 Report on the Current State of Enterprise Risk Management" which provides benchmarking data based on research conducted by the ERM Initiative at North Carolina State University on behalf of the American Institute of CPAs Business, Industry & Government Team.

(http://www.aicpa.org/InterestAreas/BusinessIndustryAndGovernment/Resources/ERM/Pages/default.aspx)

COSO

The COSO (Committee of Sponsoring Organizations of the Treadway Commission) Enterprise Risk Management – Integrated Framework (Reference Copy) provides principles-based guidance to help entities design and implement effective enterprise-wide approaches to risk management.

(http://www.coso.org/documents/Framework%20Reference%20Secured.pdf)

In addition, COSO has released a number of ERM thought papers including:

- Embracing Enterprise Risk Management: Practical Approaches for Getting Started
- Enterprise Risk Management – Understanding and Communicating Risk Appetite
- ERM Risk Assessment in Practice
- Developing Key Risk Indicators to Strengthen Enterprise Risk Management
- Effective Enterprise Risk Oversight: The Role of the Board of Directors

(http://www.coso.org/-ERM.htm)

ISO International Standards

ISO 31000:2009, Risk management – Principles and guidelines, provides principles, framework and a process for managing risk.

(http://www.iso.org/iso/home/standards/iso31000.htm)

Treasury Board Secretariat of Canada

The Treasury Board Secretariat of Canada has published its Framework for the Management of Risk, a Treasury Board policy instrument that outlines a principles-based approach to risk management for all federal organizations.

In addition, the Treasury Board Secretariat has available a number of guides and tools including:

- Guide to Integrated Risk Management
- Guide to Corporate Risk Profiles
- Guide to Risk Statements
- Guide to Risk Taxonomies
- Risk Management Capability Model

(http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/rm-gr-eng.asp)

Other Reports and Thought Papers

Other reference material includes:

- IBM Centre for The Business of Government Report on "Improving Government Decision Making through Enterprise Risk Management"

  (http://www.businessofgovernment.org/report/improving-government-decision-making-through-enterprise-risk-management)