ATTACHMENT 2

AUDITOR GENERAL'S OFFICE 2021 WORK PLAN
RISK FACTORS CRITERIA USED IN CITY-WIDE RISK ASSESSMENT

1) CYBER SECURITY AND INFORMATION AND TECHNOLOGY EXPOSURE

Given the dependence of business operations on information technology, the risks related to the availability of systems, confidentiality, and integrity of data are often considered among the top risks to organizations.

In recent years, many municipalities and other public/private sector organizations in Canada and the U.S. have been affected by cyber attacks. These cyber attacks have resulted in the loss of sensitive information and confidential data, and have caused the denial of service in a number of instances where municipalities and organizations were not able to provide services to their citizens, businesses, and other stakeholders. These cyber attacks also resulted in significant financial losses and litigation issues.

The City provides a number of services, such as information about and registration of various programs for kids, communities, and businesses through the internet. The City's IT infrastructure stores a significant amount of confidential and sensitive data, such as information about employees' and citizens' personal records. It also maintains a large number of systems that are critical to the City's operations and providing services, such as water, fire services, transportation, and emergency response to the citizens of Toronto.

Weaknesses in information technology controls could lead to potential cyber-security risks, exposing the City to compromise confidential information, or the potential shutdown of critical technology systems that are relied upon to provide services to citizens.

The following are some important factors that impact the IT security exposure of an operating unit:

- Existence of an IT Governance framework, adequacy of policies and procedures
- Security over data collection, management and storage, such as data relating to personally identifiable information, financial records including credit card information, etc.
- IT access controls, monitoring, and change management
- Pace of adoption of new technologies, comparison with industry benchmarks, and compliance with cyber-security standards
- Business continuity, applications and systems change management, and disaster recovery procedures
- Employee training and awareness on information technology and cyber security

2) LEGAL EXPOSURE (INCL. ENVIRONMENTAL, REGULATORY, LITIGATION)

Exposure to risk can be introduced by non-compliance with internal and external policy, procedure, regulatory, and statutory matters. Non-compliance can result in public embarrassment and/or monetary loss due to improper business practices, the levy of fines or litigation, loss of funding sources, disallowed costs from funding agencies, and in certain cases may compromise privacy or health and safety.

The complexity and clarity of internal / external requirements impacts an organization's ability to comply, and therefore influences the degree of exposure to risk. Compliance risk may be mitigated if external third parties / government sectors are required to perform independent monitoring / audits.

Consideration should be given to:

- Crisis management (i.e. health-related pandemics, mass public violence, natural disasters)
- People and equity (i.e. diversity and inclusion, mental health awareness, harassment)
- Climate change (i.e. reducing the carbon footprint, risks to infrastructure)
- Health and safety

3) SUSCEPTIBILITY TO FRAUD, OTHER WRONGDOING, OR WASTE

The Disclosure of Wrongdoing and Reprisal Protection policy, part of the Toronto Public Service By-law (Chapter 192), includes a duty for employees to report allegations of wrongdoing. Specifically, the By-law requires:

- all City employees who are aware that wrongdoing has occurred to immediately notify their manager, their Division Head, or the Auditor General's Office
- allegations of wrongdoing received by Division Heads, Deputy City Managers or the City Manager to be immediately reported to the Auditor General
- employees who report wrongdoing in good faith to be protected from reprisal.

Exposure to potential losses from fraud, other wrongdoing, or waste may be impacted by various factors including the degree of:

- pressure on employees to achieve performance goals
- opportunities from weak internal controls (e.g. inadequate segregation of duties) or management override of controls
- liquidity of assets
- potential conflicts of interest or collusion

Fraud and wrongdoing in the following areas have been identified in recent years:

- irregular procurement practices
- misuse of City resources
- subsidy claim fraud
- employee benefits fraud
- sick leave abuse / overtime
- conflict of interest

An effective way to deal with fraud or other wrongdoing is to identify and document fraud risks. In the consideration of risk, it is important to assess the extent of fraud or other wrongdoing that has occurred and the adequacy of fraud prevention and awareness activities. Fraud risks are not limited to theft and misappropriation of cash or physical assets, but should consider emerging trends and historic trends in the program area.

4) COMPLEXITY AND SIGNIFICANT CHANGES IN OPERATIONS AND SERVICE DELIVERY

The degree of risk is influenced by the complexity, size, scope, and magnitude of a unit's operations, activities, and service delivery. Units may deal with a high volume of transactions and/or a portfolio of programs and services of varying size and complexity, the people, process, and technology to support them, and all of the related regulations.

The complexity of a unit's operations must be considered within the context of interdependencies and agreements with third parties, (i.e. general contractors, subcontractors, housing providers, etc.), divisions, agencies, and corporations, and the City as a whole. It may be difficult to establish clear accountability for process and control ownership, and alignment of risk decisions and tolerances.

In addition, structural changes, reorganizations, changes in third-party relationships, and key management turnover can all potentially increase risks for established operations.

5) ALIGNMENT OF STRATEGIC / BUSINESS / SERVICE PLANNING

The development and implementation of strategic and long-term business plans define the key initiatives and priorities of a unit. A Division/Agency/Corporation's business plan links funding requirements to organizational goals and objectives in the short-term (annual) and for a longer-term period (three to five years).

These plans also establish the formal goals and objectives for the organization, and communicate them to staff. This allows staff to develop performance objectives which are aligned with the organizational objectives. Both personal and organizational objectives should include measurable performance targets and indicators.

Without clearly defined goals, objectives, performance measures/targets, and outcomes, it is not possible to track and evaluate the effectiveness of a unit. It is important that the outcomes set are also aligned with the City's goals and help the City to move forward. Also, without a periodic refresh, and continuously measuring outcomes, the strategic plan and business plans may lose relevance, increasing the risk that operations will not meet stakeholder expectations.

6) STAFFING LEVELS & ORGANIZATION COMPETENCE

There must be sufficient personnel with appropriate experience and capability to manage day-to-day operations in accordance with policies and procedures, make decisions, and maintain internal controls. To limit organizational exposure, these

individuals need to understand their roles and responsibilities and be accountable for their actions or lack thereof.

Changes in an organization's management personnel, structure or systems influence risk. For example:

- Reorganization of responsibilities and activities can result in significant changes that compromise the internal control environment.
- Significant downsizing, inadequate succession planning, and process reengineering efforts may also increase risks if there are inadequate protocols in place to transfer knowledge or the control environment is not carefully analyzed and preserved. For example, adequate levels of authorization balanced with adequate segregation of duties.
- Every new election may present new City Council priorities that may impact existing systems or processes.

7) FINANCIAL EXPOSURE (MATERIALITY AND IMPACT)

Large dollar amounts either flowing through a system or committed to an activity or project will increase financial risk. Any potential financial loss (impact) depends on the dollar value of revenues and / or expenditures that a program manages.

Financial risks can also impact the adequacy of City reserve and reserve fund balances which are Council-approved:

- for planned future expenditures;
- to protect the City against unbudgeted or unforeseen events;
- to smooth out future program expenditures which may fluctuate from one year to the next;
- or to accumulate funds for future capital expenditures or irregular or occasional expenses (such as municipal elections every four years).

It is also important to note that some Divisions may have relatively small operating / capital budgets but are responsible for managing or administering significant funds (i.e. Engineering and Construction Services, Accounting Services (Accounts Payable, Accounts Receivable), PPEB – Employee Benefits, Revenue Services (Property Tax Collection, Water Billings, etc.)). These represent "at risk" dollars that need to be considered when assessing financial risk.

8) CONTRACTUAL EXPOSURE

All contracts present some level of risk. Risks can be increased or mitigated by the manner in which contracts for service providers and suppliers are procured and managed. Contract risk exposure is impacted by the degree to which:

- Oversight of procurement has been centralized (i.e. through the Purchasing and Materials Management Division)
- Compliance with procurement policies
- Formal, open, competitive procurement processes are used

- Wording of contract deliverables, outcomes, and any consequences for non-performance, etc. is clearly defined and clearly understood by all parties
- Irregular purchasing activities have been identified
- Contract management practices have been implemented by knowledgeable staff
- Potential conflicts of interest have been identified and addressed

9) ADEQUACY OF POLICIES, PROCEDURES, PROCESSES AND CONTROLS

Policies and procedures should be in place so that activities efficiently and effectively support the achievement of an organization's objectives in a consistent manner. Policies and procedures need to be communicated so that staff understand what is expected of them and the scope of their freedom to act. Authority, responsibility and accountability should be clearly defined so that the appropriate people make decisions and take action.

Even if policies and procedures are well-defined, processes must be in place to monitor adherence with requirements and address instances of isolated and/or recurring non-compliance in a timely manner.

10) PUBLIC AND POLITICAL INTEREST (INCL. ADVERSE PUBLICITY)

Events can occur which erode public confidence in the City of Toronto. As the level of visibility, political and/or public interest, or potential for public embarrassment increases, the degree of exposure will increase. The amount of interest that Council expresses in a particular unit or function could also impact this factor.