ANNUAL UPDATE – INFORMATION TECHNOLOGY RISK MANAGEMENT

EXECUTIVE SUMMARY

This annual report of Information Technology (IT) Risk Management provides an overview of the IT-related risks (including measures being taken to mitigate their likelihood and/or impact). The risks identified in Attachment 1 may affect the achievement of Council's Priorities, Action Plan, and the goals of the Leadership Strategic Plan over the course of the 2015-2018 business cycle. Effective risk management will help to reduce the likelihood and/or the impact of these.

ADMINISTRATIONS RECOMMENDATION(S)

1. That Audit Committee receives this report for information.

2. That Attachment 1 remains confidential pursuant to Sections 24(1)(a) and (b) of the Freedom of Information and Protection of Privacy Act until the identified risks have been mitigated.

BACKGROUND

The Information Technology (IT) Business Unit is responsible for providing IT infrastructure, services and solutions to The City's business units. To properly manage the risks associated with the provision of these services, IT uses the Corporate Risk Management framework as mandated by the Integrated Risk Management policy.

Per direction received at the 2011 January 20 meeting of Audit Committee, and in accordance with the Audit Committee Terms of Reference Bylaw Number 48M2012, IT is to provide an annual update on information technology risk management and controls. This report provides an overview of IT's risk management strategies, including the current risk register, and shows how risk management has been embedded into IT's Action Plan.

INVESTIGATION: ALTERNATIVES AND ANALYSIS

Information technology is an industry sector with a disciplined focus on systems design, founded on principles and requirements for resiliency, redundancy and sustainability. With technology underpinning every service provided to citizens and due to the sensitivity of the data The City safeguards, our tolerance for technology-related risks is based on the principle of protecting The City's reputation and maintaining the public's trust.

IT manages risk in an integrated manner. IT looks at strategic risk through Action Plan and the Principal Corporate Risk Report and manages operational risk through the implementation of targeted programs. Given the integrated nature of risk management, IT finds the current level of risk is manageable and acceptable, with risk mitigations being integrated into current work plans, budgets and staffing resources. Strategic risks that were identified during the development of Action Plan 2015-2018 drive IT's capital investments.

Information and documentation provided within this IT risk report were obtained from the IT Management Team and IT Leaders and references ongoing IT practices. IT's Risk Register gap analysis, risk likelihoods, and impact mitigations were prioritized as part of the development of IT's 2015-2018 Action Plan and are reviewed by IT Management on a quarterly basis. The IT

ANNUAL UPDATE – INFORMATION TECHNOLOGY RISK MANAGEMENT

Risk Register was a source for the departmental Risk Register, which in turn provided input into the Annual Principal Corporate Risk Report (AC2017-0020) presented to Audit Committee on 2017 January 19.

Furthermore, in accordance with the Corporate Project Management Framework, all projects managed by IT have their own dedicated risk registers. These risks are monitored by the assigned project manager and regularly reviewed by IT's Project Management Office, the project sponsors, steering committees and IT managers. Appropriate actions are taken when required to mitigate risks to each project's quality, schedule and budget.

To support the successful delivery of software development projects, IT follows The City's Software Solutions Methodology, a set of best practices and guidelines with scalability to suit a variety of projects. Defined touchpoints ensure stakeholders across the organization are effectively engaged throughout all stages of the project lifecycle. Adherence to the Software Solutions Methodology enables quality solution delivery on a consistent basis.

Adapting to the constantly changing cyber security landscape is a top priority for both IT and Corporate Security. Accordingly, the Chief Information Technology Officer and Chief Security Officer routinely meet to discuss cyber security strategies and tactics and coordinate efforts around joint projects and solution development.

Stakeholder Engagement, Research and Communication

Every year, IT engages stakeholders from across the enterprise as part of its client satisfaction survey. Results indicate that businesses are mostly happy with the quality of the products and services offered by IT, with 91 per cent of respondents to 2016's survey indicating they were either "Very Satisfied" (44 per cent) or "Somewhat Satisfied" (47 per cent).

IT has a history of measuring and benchmarking its business, functions and associated costs. Over the past six years, IT has leveraged both the Municipal Benchmarking Network Canada (MBNCanada) and an industry benchmarking service to compare costs and services with those of other jurisdictions in Canada, other government organizations and private enterprises of similar size and complexity. The benchmarking results are then used to identify opportunities for cost-reduction or service improvement.

STRATEGIC ALIGNMENT

The City's Enterprise Architecture principles have been established to guide technology decisions and actions. Adherence to these principles helps reduce risk when making technology-related decisions. The Enterprise Architecture principles include, but are not limited to, the following:

- Flexible, modular components and artifacts shall be designed and built for re-use and shall be re-used when developing solutions;
- Preference shall be given to "re-use before purchase" and "purchase before building", taking into account business and technical requirements;
- Solution delivery shall be driven by accepted industry standard practices and methods with priority given to open system architecture characteristics;

ANNUAL UPDATE – INFORMATION TECHNOLOGY RISK MANAGEMENT

- Systems, data, transactions and networks shall be secured based on industry good practice and business requirements and shall conform to all applicable laws, regulations and policies; and,
- The enterprise strategy and architecture shall be designed to reduce diversity and minimize complexity.

The 2015 Technology Governance Model, approved by the Administrative Leadership Team, balances the desire by The City's departments and business units to make their own technology-related decisions and IT's ability to efficiently and effectively manage technology investments. IT is establishing a methodology based on Results Based Accountability for reporting benefits realized from technology investments and projects. As the Technology Governance Model matures, lines of business will have a greater understanding of the strategic alignment, risk, and operational costs their technology requests and decisions have on IT and The City.

The risks identified in Attachment 1 may affect the achievement of Council's Priorities, Action Plan, and the goals of the Leadership Strategic Plan over the course of the 2015-2018 business cycle. Effective risk management will help to reduce the likelihood and/or the impact of these.

Social, Environmental, Economic (External)
No implications to this report.

FINANCIAL CAPACITY
Information Technology's budget is developed and reported as part of The City's overall financial reporting practices.

Current and Future Operating Budget:
No implications to this report.

Current and Future Capital Budget:
No implications to this report.

RISK ASSESSMENT
Internal Audits by the City Auditor's Office
IT has been the subject of several recent internal audits and internal control reviews which have investigated operating procedures, policies and business practices. As of February 2017, IT has closed all but one audit recommendation from the City Auditor's Office. The final outstanding audit, related to the security of the PeopleSoft HCM module, will be closed during a planned system upgrade scheduled for completion in Q3 2017.

External Audit of Year-End Financial Statement
Every year, the external auditor performs an audit on The Corporation's financial statements which includes assessing processes and controls of the technology systems and the technology environment used to manage The City's finances. For Information Technology, this work is completed via interviews, observing operations and testing documented procedures against actual practices. This is not intended to be a comprehensive audit of The City's entire technology environment; however, the external auditor may find opportunities for improvement

ANNUAL UPDATE – INFORMATION TECHNOLOGY RISK MANAGEMENT

for The City's financial technology systems. IT follows industry best-practices by documenting its services, operational accountabilities and responsibilities.

As part of the annual year-end financial statement audit, the external auditor will determine if IT's current policies, practices and procedures for The City's financial technology system and technology environment satisfies all requirements of the audit. Results for the 2016 fiscal year are expected in March 2017.

Integrated Risk Management

IT works within The Corporate Integrated Risk Management program parameters to capture and monitor business and technology risk. Identified risks are assessed, managed and communicated in the IT Risk Register (Attachment 1). IT's risk mitigation strategies are incorporated into IT's Action Plan and further outlined in the corporate risk reporting framework.

IT, in partnership with Law/Corporate Security, manages cyber security risks by setting and monitoring corporate policies. As outlined in the Code of Conduct, all City of Calgary staff must take care to follow the policies and guidelines and enter into the mindset of safeguarding The City's hardware, software and information assets. A review of the Acceptable Use of City Technology Resources Policy was completed in 2016, with approval of the updated policy received from the Administrative Leadership Team in Q3 2016. In Q1 2017, there is a corporate communications campaign about the Code of Conduct (including the Acceptable Use of City Technology Resources Policy).

As listed in the 2017 Annual Principal Corporate Risk Report (AC2017-0020), technology security continues to be an area requiring ongoing research and education by both IT and Law/Corporate Security. In order to understand the changing nature of this risk exposure and potential likelihood and impacts to The City technology environment, IT and Law/Corporate Security work closely together to monitor, test and improve The City's cyber defences. Crisis management plans are in place should an incident occur.

Control Environment Assessment Audit

Audit Committee Bylaw 48M2012 assigns responsibility to the Audit Committee for overseeing the integrity of The City's system of internal controls. The annual assessment is based on the COSO Internal Control – Integrated Framework; consisting of five inter-related components and 17 principles. For The City's system of internal controls to be deemed effective, all five components and all 17 principles must be present and functioning as intended. IT is either solely or jointly responsible for several of these components and principles and is contributing extensively to the 2017 audit which is currently in progress.

Highlighted Risks

In accordance with Integrated Risk Management best practices, the IT Management Team reviews and updates the IT Risk Register on a quarterly basis and ensures that appropriate actions are being taken to manage identified risks. As of the last management review (February 2017), IT has identified seven risks with an assessment rating of High-High, High-Medium, or Medium-High for "likelihood" and "impact", respectively. Information regarding each of these risks – in addition to those that have been assessed with lesser severity ratings – and the on-

ANNUAL UPDATE – INFORMATION TECHNOLOGY RISK MANAGEMENT

going and planned actions to mitigate likelihood and impact can be found in Attachment 1: IT Risk Register.

REASON(S) FOR RECOMMENDATION(S):
Audit Committee has internal control and risk management oversight responsibilities of Information Technology.

ATTACHMENT(S)
1. IT Risk Register