Chief Financial Officer's Report to
Audit Committee
2018 February 13

ISC: UNRESTRICTED
AC2018-0133

Annual Update – Information Technology Risk Management

EXECUTIVE SUMMARY

This annual report of Information Technology (IT) Risk Management provides an overview of technology-related risks, including measures being taken to mitigate their likelihood and/or impact. IT manages strategic, project, and operational risk in a manner to ensure the systems that support all City services are functional, secure, and resilient. A detailed description of each IT risk and associated mitigation techniques can be found in Attachment 1.

ADMINISTRATION RECOMMENDATION:

That Audit Committee:

1. Receive this Report for information; and
2. Keep Attachment 1 confidential pursuant to Section 24 of the *Freedom of Information and Protection of Privacy Act* until the identified risks have been mitigated.

PREVIOUS COUNCIL DIRECTION / 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 and demonstrates how risk management has been embedded into IT's Action Plan.

BACKGROUND

The IT business unit serves City employees, civic partners, and citizens by provisioning, managing, and governing the use of technology solutions and associated infrastructure. IT uses the Corporate Risk Management Framework as mandated by the Integrated Risk Management Policy (CC011) to properly manage the risks associated with City technology.

INVESTIGATION: ALTERNATIVES AND ANALYSIS

Our world is changing dramatically, and no sector is affected more by the fast rate of change than technology. Recent years have seen unprecedented advancement in the fields of machine learning, artificial intelligence, virtual reality, augmented reality, and robotics. Leveraging new technologies while maintaining existing systems and securing The City's assets against new and emerging cyber threats remains a constant challenge for IT.

Every service provided to citizens and City employees includes a technology component in some form. In accordance with IT industry best practices, The City's hardware and software solutions are designed with resiliency, redundancy, and sustainability as top considerations. The City collects, processes, and stores many terabytes of data on behalf of citizens, so protecting our reputation and maintaining the public's trust is a high priority for IT. Effective management of technology-related risks is critical to The City's business continuity plans.

IT's Risk Register, including risk likelihoods, impacts, and planned mitigation strategies, is reviewed by the IT Management Team on a quarterly basis. The IT Risk Register is one of several departmental and business unit risk registers that was rolled up into the Annual Principal Corporate Risk Report (AC2018-0066) presented to Audit Committee on 2018 January 26.

In consultation with the IT Management Team and the Chief Security Officer, the Chief Information Technology Officer has determined that existing controls and work plans for improvement activities described in Attachment 1 are manageable. Ongoing mitigation techniques for strategic and operational risks are integrated into IT methodologies, work plans, budgets, and staffing resources. IT's capital investments are driven, in part, to address strategic risks that were identified during the development of Action Plan 2015-2018.

Stakeholder Engagement, Research and Communication

IT invites City of Calgary employees from all levels of the organization to provide performance feedback via the annual IT Client Satisfaction Survey. Overall satisfaction has remained high for several consecutive years, 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) with the products and services delivered by IT. Data collection for the 2017 Client Satisfaction Survey was completed in 2018 January, and the final report is expected in 2018 February.

IT uses an industry-leading benchmarking service to compare its business, functions, and associated costs with other public and private sector organizations of similar size and complexity. The results are used to highlight areas where The City compares favourably to our peers and to identify opportunities to improve service delivery and cost efficiency. IT is also a contributing member to the Municipal Benchmarking Network Canada expert panel. These benchmarking activities serve as inputs into IT's current Zero-Based Review.

Strategic Alignment

Technology security remains one of the top concerns of The City. In recent years, there have been several high-profile cyber security attacks targeting Canadian organizations such as the University of Calgary (ransomware), MacEwan University (phishing), and Bell Canada (breach of customer data). Protecting The City against these and other technology security threats is a shared responsibility of IT and Corporate Security, as described in the 2018 Annual Principal Corporate Risk Report (AC2018-0066). The Chief Information Technology Officer and the Chief Security Officer routinely meet to review The City's cyber security systems and make plans to protect against emerging threats. Continuous research and education is necessary to understand the changing nature of this risk exposure and the likelihood and impact to The City's technology environment and reputation should a successful attack occur. IT and Corporate Security work closely together to monitor, test, and improve The City's cyber defences. An IT Crisis Management plan is in place and regularly tested. Staff are trained and prepared to put the plan into action in the event of a large system outage or security incident.

It is the responsibility of every employee to follow the policies and guidelines outlined in the Code of Conduct to safeguard The City's hardware, software, and information assets. An update to the Acceptable Use of City Technology Resources Policy was approved in 2016, and an update to the Information Management and Security Policy was approved in 2018 January. Employee education and awareness related to information management and security is essential. Code of Conduct training is currently being updated and will be rolled out to City employees in 2018.

The 2015 Technology Governance Model (ALT 2014-0936) balances the desire of The City's departments and business units to make technology investment decisions with IT's ability to efficiently and effectively manage technology investments. 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 have on IT and The City. Most City departments have already established or are in the process of establishing technology committees and developing terms of reference for guiding technology investments. This work is being done in preparation for prioritizing technology investments during the One Calgary 2019-2022 business cycle. The Corporate Technology Committee (CTC) provides strategic leadership for this work which is targeted for completion by the end of 2018. CTC recently approved the Corporate Technology Plan and Enterprise Platform to set standards and guide decision-making.

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;
- 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.

In accordance with the Corporate Project Management Framework, technology projects managed by IT have their own dedicated risk registers maintained by the assigned project manager. These are regularly reviewed by IT's Project Management Office, project sponsors, steering committees, and IT managers to ensure appropriate actions are taken when necessary to mitigate risks to each project's quality, schedule, and budget.

IT created the Software Solutions Methodology (SSM) for software development projects. The SSM is a set of best practices and guidelines to ensure stakeholders across the organization are effectively engaged throughout all stages of the project lifecycle. Adherence to the SSM enables quality solution delivery on a consistent basis, and it is scalable to suit projects of many different sizes and scopes.

Social, Environmental, Economic (External)

No implications to this report.

Financial Capacity

IT'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

The risks identified in Attachment 1 may affect the achievement of Council's Priorities and Action Plan over the course of the 2015-2018 business cycle. Effective risk management reduces the likelihood and/or the impact of these.

Internal Audits by the City Auditor's Office

Over the past few years, the IT business unit has been the subject of multiple audits and control reviews initiated by the City Auditor's Office. Four recommendations are currently open as of 2018 January. One recommendation (AC2013-0446 Recommendation 14.1) concerns enhanced security of the PeopleSoft system and will be resolved by mid-2018. The remaining three recommendations (AC2017-0590 Recommendations 1, 4, and 5) are follow-up activities from previously completed audits and are expected to be closed by the end of 2018.

External Audit of Year-End Financial Statement

The Corporation's financial statements and records are audited by the external auditor each year. A prerequisite of this audit is an assessment of the internal processes and controls related to the technology systems used to manage and report The City's finances. The external auditor observes IT operations, conducts interviews with IT subject matter experts, and tests our actual practices against our approved and documented procedures. While this is not intended to be a comprehensive audit of The City's entire technology environment, the external auditor may identify opportunities to improve the processes and controls used to manage and secure The City's financial systems. The fiscal year 2017 assessment is currently in progress, and assessment findings are expected in 2018 February.

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. The top risks in the IT Risk Register are then rolled into the Chief Financial Officer's Department Risk Register and Annual Principal Corporate Risk Report.

Annual Update - Information Technology Risk Management

Control Environment Assessment

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. For The City's system of internal controls to be deemed effective, all components and principles must be present and functioning as designed. IT is either solely or jointly responsible for several of these components and principles and is contributing extensively to the current assessment which is scheduled for presentation to Audit Committee on 2018 April 17.

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 (2018 January), IT has identified two risks with an assessment rating of High/Red. Information regarding all IT risks and the on-going and planned actions to mitigate likelihood and impact can be found in Attachment 1.

REASON(S) FOR RECOMMENDATION(S):

Audit Committee has internal control and risk management oversight responsibilities of Information Technology.

ATTACHMENT(S)

1. Information Technology Risk Register (Confidential)
2. Information Technology Risk Management Presentation