

Chief Financial Officer's Report to
Audit Committee
2019 July 23

ISC: UNRESTRICTED
AC2019-0945

Annual Update – Information Technology Risk Management

EXECUTIVE SUMMARY

Each year, Information Technology (IT) provides an annual report on the technology-related risks within The City and the measures being taken to mitigate their likelihood and/or impact. IT reviews and manages risks to ensure that systems supporting all City services remain 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 Sections 24(1)(a) and (b) of the Freedom of Information and Protection of Privacy Act; to be reviewed in 2024 July.

PREVIOUS COUNCIL DIRECTION / POLICY

As directed 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 daily operations.

BACKGROUND

The IT business unit is responsible for provisioning, managing, and governing the use of technology, services, and solutions used by City employees, civic partners, and citizens. To properly manage the risks associated with City technology, IT uses the Integrated Risk Management Framework as mandated by the Integrated Risk Management Policy (CC011).

INVESTIGATION: ALTERNATIVES AND ANALYSIS

Each of the 61 services at The City of Calgary relies on technology in order to deliver internal and citizen-facing services. Managing technology-related risks to protect The City's reputation and maintain the public's trust is critical.

As the pace of technology change accelerates, IT is continually reviewing emerging trends to determine where to invest. Ensuring that there are appropriate business cases for technologies such as the Internet of Things is critical to ensure investments offer sufficient benefits to service delivery.

In order to help monitor and manage risks, IT uses a Risk Register to capture risks and takes into consideration their likelihood, impact, and planned mitigation strategies. The IT Risk Register is reviewed by the IT Management Team on a quarterly basis. Information in the Risk Register is used to populate the Chief Financial Officer's Department risk summary and the Annual Principal Corporate Risk Report presented to Audit Committee on 2019 January 31 and 2019 July 23.

**Chief Financial Officer's Report to
Audit Committee
2019 July 23**

**ISC: UNRESTRICTED
AC2019-0945**

Annual Update - Information Technology Risk Management

The IT Management Team, Chief Security Officer, and Chief Information Technology Officer collaborate to ensure 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 the One Calgary 2019-2022 business plan and budget.

Stakeholder Engagement, Research and Communication

On an annual basis, IT conducts a client survey enabling employees to evaluate the performance of the work IT does and to share their level of customer satisfaction. Overall satisfaction has remained high for several consecutive years. In 2018, 92 per cent of survey respondents indicating they were satisfied with their experiences with the IT business unit within the past year, including 48 per cent who have indicated they were very satisfied. Data for the most recent Client Satisfaction Survey was collected 2019 June and the final report is expected 2019 July. A moderate decline in client satisfaction is anticipated due to consolidated workforce productivity devices, rationalized business software titles, and reduced service levels for less-critical IT functions.

IT leverages information from Municipal Benchmarking Network Canada and an industry-leading benchmarking service to compare The City's IT services and costs with other public and private-sector organizations. The most recent benchmarking study highlighted that The City is investing more in IT than its peers, but is managing this investment efficiently.

The Client Satisfaction Survey and the annual benchmarking studies are used to identify where The City is performing favorably and where there are opportunities to improve service delivery or cost efficiency.

Strategic Alignment

Cyber security remains a top concern of The City, as identified in the 2019 Annual Principal Corporate Risk Report (AC2019-0032). Continuous research and education are necessary to understand and adapt to the changing nature of this risk exposure. IT and Corporate Security work closely together to monitor, test, and improve The City's cyber defences to protect against emerging threats. IT's Crisis Management plan was reviewed and tested in 2019 to ensure staff are prepared to respond in the event of a large system outage or security incident.

Employee education and awareness are key components of safeguarding The City's information and technology assets. The Acceptable Use of City Technology Resources was updated in 2016. The Information Management and Security Policy and associated standards (Access and Sharing, Electronic Communications, Information Security Classification, and Intellectual Property) were updated in 2018. Code of Conduct training was rolled out to staff 2018 June. Workshops on Information Management and Security and online training for Information Security Awareness are available to staff on an ongoing basis.

**Chief Financial Officer's Report to
Audit Committee
2019 July 23**

**ISC: UNRESTRICTED
AC2019-0945**

Annual Update - Information Technology Risk Management

The Corporate Technology Committee (CTC) governs the risk and impact of corporate technology investments at The City. As identified in the 2015 Technology Governance Model (AC2014-0936), The City is moving towards a federated governance model. Most City departments have already established or are in the process of establishing technology committees and developing terms of reference for guiding technology investments. The CTC Terms of Reference was updated in 2018 to reflect and clarify the role of the CTC within the federated governance model.

The Corporate Technology Plan was updated in 2018 and defines current and future corporate technology strategies, standards, and direction that help guide The City's business units in their technological decision-making. The Corporate Technology Plan is sponsored by the CTC and supports the corporate technology governance model.

The recently-completed IT Zero-Based Review (ZBR) assessed services and identified specific opportunities for improvements to efficiency and effectiveness. The Right Device opportunity is working to optimize the use of personal productivity devices throughout The City to ensure each user has the right device to their job. The Application Portfolio Management opportunity is focusing on reducing The City's technology debt, decommissioning applications, and rationalizing the application portfolio.

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.

In accordance with the Corporate Project Management Framework, technology projects managed by IT have dedicated risk registers which are regularly reviewed by the IT project manager, IT's Project Management Office, project sponsors, steering committees, and IT managers to ensure appropriate actions are taken to mitigate project risks.

The IT Software Solutions Methodology for software development projects is a set of best practices and guidelines to ensure stakeholders across the organization are effectively engaged throughout all stages of the project lifecycle.

Social, Environmental, Economic (External)

Effective management of technology risks ensures systems supporting all City services remain functional, secure, and resilient in order to delivery internal and citizen-facing services.

Financial Capacity

Current and Future Operating Budget:

None related to this report.

Current and Future Capital Budget:

None related to this report.

Risk Assessment

The risks identified in Attachment 1 may affect the achievement of Council's Priorities and IT's strategies over the course of the 2019-2022 business cycle. Effective risk management reduces the likelihood and/or the impact of these risks.

**Chief Financial Officer's Report to
Audit Committee
2019 July 23**

**ISC: UNRESTRICTED
AC2019-0945**

Annual Update - Information Technology Risk Management

Internal Audits by the City Auditor's Office

Over the past few years, the IT business unit has been the subject of multiple audits by the City Auditor's Office. IT has one outstanding recommendation related to the Open Data Program (AC2018-1008). IT has been identified as a stakeholder / contributor to two remaining recommendations for the Cyber Security Incident Response Audit (AC2018-0410). All outstanding recommendations are expected to be completed by the end of 2019.

External Audit of Year-End Financial Statement

As part of The City's annual external audit, internal processes and controls related to the IT environment are assessed. The external auditor conducts interviews with IT subject matter experts, observes IT operations, and tests IT practices against approved and documented procedures. The assessment for the fiscal year 2018 was completed in February 2019 and all risks related to the identified deficiencies were addressed.

Integrated Risk Management

As mandated in the Integrated Risk Management Policy (CC011), IT identifies and manages risks using the Integrated Risk Management Framework. Risks are analyzed, evaluated, monitored, and managed using the IT Risk Register. The top risks in the IT Risk Register are highlighted in the Chief Financial Officer's Department risk summary and rolled-up into the Principal Corporate Risk Report.

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 five inter-related components and 17 principles outlined in the COSO Internal Control – Integrated Framework. IT is responsible for several principles within the framework and contributes to the annual assessment. The results of the most recent assessment were presented to Audit Committee on 2019 April 23 (AC2019-0529).

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. In 2019, a new 5 x 5 matrix was introduced to evaluate the likelihood and impact of risks. As of the last management review 2019 April, IT identified one risk with a rating of Extensive and nine risks with a rating of High. Information regarding IT risks, existing controls, 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. Attachment 1 – Information Technology Risk Register - CONFIDENTIAL
2. Attachment 2 – Information Technology Risk Management Presentation