INFORMATION TECHNOLOGY (IT) FOLLOW-UP AUDIT

EXECUTIVE SUMMARY

The City Auditor's Office (CAO) issued the Information Technology (IT) Follow-Up Audit Report to Administration on July 14, 2017. The report includes Administration's response to five recommendations raised by the CAO to further reduce risk exposure. Administration accepted all recommendations and has committed to the implementation of action plans no later than December 31, 2018. The CAO will track the implementation of these commitments as part of our on-going follow-up process.

RECOMMENDATIONS:

1. That Audit Committee receive this report for information;
2. That Audit Committee recommend that Council receive this report for information; and
3. That Audit Committee recommend that Attachment to Report AC2017-0590 remain confidential pursuant to Sections 20(1)(k) and (m) of the *Freedom of Information and Protection of Privacy Act until the year 2032.*

PREVIOUS COUNCIL DIRECTION / POLICY

Bylaw 30M2004 (as amended) established the position of City Auditor and the powers, duties and functions of the position. Under the City Auditor's Office Charter, the City Auditor presents an annual risk-based audit plan to Audit Committee for approval. The City Auditor's Office 2017/18 Annual Audit Plan was approved on November 10, 2016. The City Auditor is accountable to Council and subject to the oversight of Audit Committee under Bylaw 48M2012 (as amended).

BACKGROUND

This audit was undertaken as part of the approved City Auditor's Office 2017/18 Annual Audit Plan. The objective of this audit was to assess the effectiveness of management's actions to mitigate business risks in response to CAO audit recommendations raised over the last five years. The follow-up audit focused on these past audits:

- AC2013-0085 - Technology Investment Governance;
- AC2013-0446 - PeopleSoft HCM Application Security;
- AC2013-0447 - Corporate Technology IT Network Access Security;
- AC2014-0162 - Virtual Server Security; and
- AC2015-0205 - Virtual Desktop Infrastructure.

We evaluated the effectiveness of current status implementation of management actions through the assessment of risk mitigation approaches, residual risk exposure, and, where appropriate, raised opportunities to mitigate undesired risks.

INVESTIGATION: ALTERNATIVES AND ANALYSIS

This audit conducted a follow-up of nine management actions that were deemed high risk due to the nature of changing or new technology, recently established IT investment governance model and IT security governance.

INFORMATION TECHNOLOGY (IT) FOLLOW-UP AUDIT

Recognizing the changing nature of new technology and IT governance model, the CAO conducted this follow-up audit to determine if the implementation of action plans in response to CAO audit recommendations raised over the last five years effectively addressed the risks identified in the audits.

We assessed five of the nine management actions as effectively implemented to mitigate the business risks. For the remaining four management actions, five recommendations were raised to support further timely risk mitigation.

Stakeholder Engagement, Research and Communication
This audit was conducted with Information Technology and Corporate Security acting as the principal audit contacts within Administration.

Strategic Alignment
Audit reports assist Council in its oversight of the City Manager's administration and accountability for stewardship over public funds and achievement on value for money in City operations.

Social, Environmental, Economic (External)
N/A

Financial Capacity
Current and Future Operating Budget:
N/A

Current and Future Capital Budget:
N/A

Risk Assessment
The activities of the CAO serve to promote accountability, mitigate risk, and support an effective governance structure. We used a risk-based approach to select key recommendations from the previous IT audits completed in the last five years.

REASONS FOR RECOMMENDATIONS:
Bylaw 48M2012 (as amended) states: "Audit Committee receives directly from the City Auditor any individual Audit Report and forwards these to Council for information."

The *Freedom of Information and Protection of Privacy Act* states:
20(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to
(k) facilitate the commission of an unlawful act or hamper the control of crime,
(m) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

ATTACHMENT
AC2017-0590 INFORMATION TECHNOLOGY (IT) FOLLOW-UP AUDIT