Audit Committee Report

DATE: Tuesday, May 28, 2024 **WARD(S):** ALL

TITLE: INFORMATION TECHNOLOGY SECURITY AUDIT UPDATE

FROM:
Michael Coroneos, Deputy City Manager, Corporate Services and Chief Financial Officer

ACTION: FOR INFORMATION

Purpose
To communicate the update of the Information Technology (IT) Security Audit.

Report Highlights
- The Office of the Chief Information Officer (OCIO) is responsible for managing the effective delivery of technologies and services to achieve the organization's objectives. The Office is responsible for the engineering, architecting, security, maintenance, implementation and support of city-wide technology and communications infrastructure.
- A co-sourced IT Security Audit was performed in 2021. The audit report was submitted to the Audit Committee on March 31, 2021.
- Management has implemented all action plans which addressed the recommendations outlined in the audit report. OCIO will deliver an update to the Audit Committee in a closed session.

Recommendation
1. That the IT Security Audit Update Presentation be received in a closed session.

Background
The Office of the Chief Information Officer (OCIO) is responsible for managing the effective delivery of technologies and services to achieve the organization's objectives. The Office is responsible for the engineering, architecting, security, maintenance, implementation and support of city-wide technology and communications infrastructure. OCIO's vision is "Making Vaughan Better for People in our Digital Age".

Securing computerized data and information is important for several reasons, but principally as a means of keeping information safe. The importance of computer security depends on how harmful it can be if data or information is lost. The City stores a lot of data, some of it very sensitive, including payment information, staff records, e-mails, citizen information and extensive corporate documents, both finished and those in progress.

In addition to security breaches by outsiders, there is also an increasing risk that data and systems can be compromised by staff inside organizations. As part of their daily responsibilities, staff have access to data and information that those outside of the organization typically do not. Although not a risk unique to computerized information, the ease of availability and accessibility to computerized information may increase the likelihood of a security breach.

An IT Security Audit was performed in 2021. The objective of the audit was to evaluate the adequacy and effectiveness of the internal controls, processes and procedures in place to mitigate the business risks associated with the management and administration of IT Security.

This audit was co-sourced. Internal Audit worked with iPSS incorporated (iPSS), who were the successful bidder after a competitive procurement process.

A number of findings were put forth to further improve existing controls as well as introduce additional controls to support the defense-in-depth principle that calls for a multi-layer defense strategy that can contribute to a more resilient and secure IT infrastructure.

Additional IT security controls as well as enhancements to existing controls have been implemented since the original assessment to ensure security of City's IT infrastructure and data.

Previous Reports/Authority

The following is a link to a previous report regarding "Information Technology Security Audit":
March 31, 2021 Audit Committee Meeting (Item 4, Report No.4)

Analysis and Options

Not applicable.

Financial Impact

There are no direct economic impacts associated with this report.

Broader Regional Impacts/Considerations

Not applicable.

Conclusion

OCIO led remediation efforts outlined in the management action plan while capturing all remediation evidence in a dedicated report.

OCIO worked with Internal Audit to validate remediation evidence and timelines to ensure tracking accuracy.

Attachments

1. Confidential Attachment – IT Security Audit Update.

Prepared by

Sergey Kanayev, IT Infrastructure and Chief Security Officer, ext. 8403.