Committee of the Whole (2) Report

DATE: Tuesday, November 12, 2019 **WARD(S):** ALL

TITLE: INTERNAL AUDIT REPORT – INFORMATION TECHNOLOGY RISK ASSESSMENT

FROM:
Kevin Shapiro, Director of Internal Audit

ACTION: FOR INFORMATION

Purpose
To present the Internal Audit Report on the Information Technology Risk Assessment.

Report Highlights
- The 2019 Internal Audit Risk Based Work Plan included an Information Technology Risk Assessment.
- The objective of the risk assessment was to rank risk factors based on the likelihood of occurrence and impacts and will help inform a multi-year IT audit work plan.
- IT audits can help the City determine whether identified risks have been mitigated, corporate policies and procedures are implemented as designed and systems can be relied upon.
- The IT Audit Plan will be integrated into the annual Internal Audit Risk Based Work Plans for the remainder of this Term of Council.

Recommendations
1. That the Internal Audit Report on the Information Technology Risk Assessment be received.

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".

According to the Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Audit and the City's Internal Audit Policy, Internal Audit has a responsibility to develop an audit work plan that reflects the current and emerging risks within the City.

The 2019 Internal Audit Risk Based Work Plan included an IT audit project. The project selected was an in-depth risk assessment of IT operations across the City. The objective of the risk assessment was to rank risk factors based on the likelihood of occurrence and impacts and will help inform a multi-year IT audit work plan.

In developing the potential objective and scope for this project, we considered areas such as:

- IT operating environment, structure and model.
- Business processes supported by IT and the IT components involved.
- Related regulations, rules, policies and procedures.
- Risk scenarios that could potentially impact the achievement of strategic and business objectives, and the mitigating controls.

Organizations have become increasingly dependent on computerized information systems to carry out their operations and to process, maintain and report essential information. As a result, the reliability of computer-generated data is a major concern to organizations. Information Technology audits can help the City determine whether identified risks have been mitigated, corporate policies and procedures are implemented as designed and systems can be relied upon.

The absence of a well-controlled IT environment can have several adverse consequences, including higher levels of loss or theft of sensitive information, unauthorized access to information and applications, loss of control over sensitive business information and theft of devices. Any one of these risks can affect the reputation of the City.

An IT audit can determine whether the information systems are safeguarding assets, maintaining data integrity, and operating effectively and efficiently to achieve the organization's goals and objectives. It is the role of Internal Audit, with the assistance of technology audit experts, to assist management in these activities to improve the control, monitoring, and response to business risks.

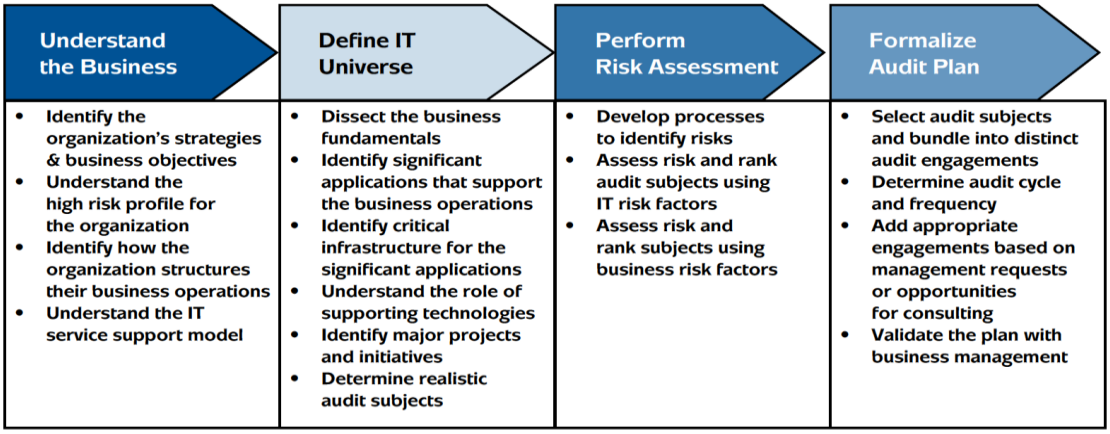
Previous Reports/Authority

Not Applicable

Analysis and Options

The Committee of Sponsoring Organizations (COSO) defines risk assessment as a dynamic and iterative process for identifying and analyzing risks to achieving the entity's objectives, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives. In the context of IT risk, a risk factor is an observable or measurable indicator of conditions or events that could adversely affect the City's IT operations and confidentiality, integrity and availability of data, which may hinder the City's ability to achieve its strategic and business objectives.

According to the IIA's Global Technology Audit Guide (GTAG) – Developing the IT Audit Plan and Guide to the Assessment of IT Risk (GAIT) for Business and IT Risk, development of IT risk assessment and audit plan should follow this process:



Among the first steps in creating the risk assessment model was to understand the City's business and operating environment. Then with the assistance from the Office of the Chief Information Officer (OCIO), Internal Audit defined the City's IT audit universe, which is a listing of all the City's significant IT assets, including applications, database, operating systems, network and data, together with the IT support and development processes.

The next step in creating the risk assessment model was to identify and rank the major inherent risks associated with each of the City's significant IT assets and processes. Inherent risk can be defined as the probability of loss arising out of circumstances or existing in an environment, in the absence of any action to control.

Through reviewing documents and interviewing stakeholders, Internal Audit assessed threats and vulnerabilities that may impact the City's IT operations, assets and data. Internal Audit identified 54 risk factors/scenarios that may affect the City's ability to

achieve its strategic objectives. For each of these risk scenarios, Internal Audit assessed its likelihood of occurrence and the impacts should it occur.

Each of the risk scenarios were ranked (i.e. low, low/medium, medium/high and high), according to the assessment combining likelihood and impact, from high to low. Based on the risk assessment methodology:

- 7 risk scenarios, or 13% were identified as having a high inherent risk rating.
- 28 risk scenarios, or 52%, were identified as having a medium/high inherent risk rating.
- 11 risk scenarios, or 20%, were identified as having a medium inherent risk rating.
- 6 risk scenarios, or 11%, were identified as having a medium/low inherent risk rating.
- 2 risk scenarios, or 4%, were identified as having a low inherent risk rating.

A high, or medium/high inherent risk rating does not imply that the risk factor is being managed ineffectively or that a process is not functioning properly

High risk areas may indicate opportunities to address activities which are mission critical and highly relevant to strategic and business objectives, have significant legal or reputation impacts, provide substantial support for other internal City operations, reflect high public need, or consume significant resources. The overall results identify the activities with the highest risk factors that may warrant and benefit from additional management action or audit services.

During the process of IT risk assessment, information from various sources were used for determining risk and work plan priorities. These include:

- Authoritative guidance from professional associations.
- City's IT strategic plans, roadmaps and documentation.
- City’s IT governance documentations, policies, standards and procedures.
- IT consultant reports on the City's IT and data governance, systems, processes and applications.
- Technology risks identified in previous audits and investigations.
- Current and emerging risks in the local government sector.

- High profile issues in other municipalities.

- Information provided by and discussions with stakeholders, including plans, policies, procedures, analysis and representation.

- Significant IT projects and initiatives.

Defining the IT audit universe and performing a risk assessment are precursor steps to selecting what to include in the IT audit plan

As the last step of the process, following assessing and rating risk scenarios, Internal Audit identified the mitigating controls for each of these risk scenarios, and develop audit plans to examine the design and operating effectiveness of these controls. During this process Internal Audit took into consideration the following factors:

- Maturity of IT operation and risk management model.
- Internal audit resources.
- Accommodating stakeholder requests.
- Integration with overall internal audit plan.

The IT Audit Plan will be integrated into the annual Internal Audit Risk Based Work Plans for the remainder of this Term of Council, and therefore, is created within the constraints of Internal Audit's operating budget and available resources. For the purposes of creating an IT Audit Work Plan, several of the 54 scenarios have been consolidated in order to create efficiencies for the purposes of conducting future audits.

As technology continues to change, so does the arrival of new and potential risks, vulnerabilities, and threats to the organization. In addition, technological changes may prompt a new set of IT goals and objectives, which in turn leads to the creation of new IT initiatives, acquisitions, or changes to meet the organization's needs. As a result, the IT audit plan priorities will be subject to periodic reviews and reassessment.

The scope of this IT risk assessment and audit plan focuses on the risks that surround, and the related controls (usually referred to as IT general controls, or ITGCs) that apply to all systems components, processes, and data present in the City and systems environment. The objectives of these controls are to ensure the appropriate development and implementation of applications, as well as the integrity of program and data files and of computer operations.

Application controls relate to the transactions and data pertaining to each computer-based application system. They are specific to each individual application. The objectives of application controls are to ensure the completeness and accuracy of records, as well as the validity of the entries made to each record, as the result of program processing. In other words, application controls are specific to a given application, whereas ITGCs are not.

According to GTAG – Developing the IT Audit Plan, there is a growing consensus among internal audit functions that business applications should be audited with the business processes they support. This provides assurance over the entire suite of controls — automated and manual — for the processes under review, helps to minimize gaps and overlaps of audit efforts, and minimizes confusion over what was included in the scope of the engagement.

The table below outlines the priority IT projects that will be proposed for approval in the upcoming annual Internal Audit Risk Based Work Plans for the remainder of this Term of Council:

Audit Project	Rationale and Risks	Strategic Plan Area of Focus
Information Technology Security Audit	**Rationale:** Securing computerized data and information is important for several reasons, but principally as a means of keeping information safe. The importance of computer security lies in 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. **Risk:** 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.	**Operational Performance and Citizen Experience**
IT Governance Audit	**Rationale:** IT governance provides a structure for aligning IT strategy with business strategy. It provides a framework of best practices and controls. By following a formal framework, the City can produce measurable results toward achieving the Term of Council Priorities and strategic objectives. **Risk:** The City requires sufficient, competent and capable IT resources in order to help the City deliver on the Term of Council Priorities and execute on the activities required to meet current and future strategic objectives. The absence of effective administration, stewardship and metrics to track initiatives can result in lost opportunities and reputational damage to the City.	**Good Governance and Operational Performance**

Audit Project	Rationale and Risks	Strategic Plan Area of Focus
Payment Card Industry Data Security Standard Compliance Audit	**Rationale:** The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that organizations that accept, process, store or transmit credit card information maintain a secure environment. The standard was created to increase controls around cardholder data to reduce credit card fraud. Since the City stores and processes payment card information in its daily operations, management needs to ensure that the City is compliant to these standards. **Risk**: In addition to non-compliance to PCI DSS, if credit card information is not secured, there is a greater risk that the information may be compromised.	**Operational Performance and Citizen Experience**
Data Management Audit	**Rationale:** According to the City's Data Management (DM) Strategy, our vision is a secure, data-rich environment accessible through a planned, collaborative and well-integrated enterprise approach to data management. This environment will be supported by an organizational culture that values and encourages mature, measured and managed data governance practices and high-quality data to enable the effective and efficient delivery of services through evidence-based decisions. **Risk:** The absence of effective administration, stewardship and metrics to track initiatives can result in not having the necessary hardware, databases and software solutions that will allow the City to monitor performance and predict future trends and conditions, which can impact the ability to make evidence-based decisions.	**Operational Performance and Citizen Experience**

During the process of the IT risk assessment, Internal Audit identified risk scenarios that have not only IT implications, but also organization-wide impacts. These risk scenarios warrant separate, broader audit attention.

Such audits may include, but not be limited to:

- Emergency Planning, Business Continuity and Disaster Recovery Audit
- Privacy Compliance Audit
- AODA Compliance Audit
- Records Management Audit
- Financial Planning and Budgeting Process Audit

Such findings are consistent with Internal Audit's entity-wide risk assessment and complement the overall risk-based audit workplan.

Financial Impact

Not Applicable

Broader Regional Impacts/Considerations

Not Applicable

Conclusion

The IT Audit Plan has been developed using the best available information and is aligned with the City's Term of Council Service Excellence Strategy Map.

The IT Audit Plan will be integrated into the annual Internal Audit Risk Based Work Plans for the remainder of this Term of Council.

For more information, please contact: Kevin Shapiro, Director of Internal Audit, ext. 8293

Attachments

Not Applicable

Prepared by

Kevin Shapiro, Director of Internal Audit, extension 8293
Hemingway Wu, Audit Project Manager, extension 8350