Office of the City Auditor

1200, Scotia Place, Tower 1
10060 Jasper Avenue
Edmonton, Alberta T5J 3R8

edmonton.ca/auditor

Information Technology General Controls – Risk Management

November 14, 2016

The Office of the City Auditor conducted this project in accordance with the *International Standards for the Professional Practice of Internal Auditing*

Information Technology General Controls – Risk Management

Table of Contents

This page is intentionally blank.

Information Technology General Controls – Risk Management

1 Introduction

The City's Information Technology (IT) systems are relied upon by every area of the City's operations. In order to govern and manage IT risks at an acceptable level, the IT Branch implemented a formal Risk Management Program in 2016.

The Office of the City Auditor 2016 Annual Work Plan included an audit of IT General Controls – Risk Management, to assess the effectiveness of controls related to the IT risk management process.

2 Background

City of Edmonton Risk Management

Effective March 1, 2016, City Council approved Policy #C587 – Enterprise Risk Management. Part of this policy requires the City Manager to:

> Develop a comprehensive Enterprise Risk Management (ERM) framework that will be followed by the City's employees for the purpose of proactively, and on an ongoing basis, identifying, evaluating, managing, mitigating and reporting on enterprise risks associated with City business or strategic goals.

The related Administrative Procedure requires the following steps to be performed:

- Establish risk context of the risk assessment process and its scope
- Identify risks
- Analyze risks
- Evaluate the likelihood and impact of those risks
- Treat risks based upon risk tolerance levels

The overall ERM process is managed by the Corporate Strategic Planning Branch. Individual Deputy City Managers are responsible to maintain registers of the risks for which their department is responsible.

Beginning in 2015, the IT Branch undertook development of the IT Risk Management Strategy and related IT Risk Management Program. This Program outlines the specific approach that will be taken with regards to IT risks faced by the City. IT risks will still be put into the City-wide ERM process; however, there is also value in reporting IT risks separately from the ERM reporting that currently takes place, due to the vast involvement of the IT systems in City operations.

IT Risk Management

The City needs to assess and manage risks such as hacking attempts, viruses and other malware, equipment obsolescence, and environmental threats that can impact the reliability of data centres and systems. These risks need to be appropriately managed so that City operations are not exposed to loss of financial data, compromised personal and citizen information, disruption of services, fraud, or other negative impacts.

The number of cyberattacks has increased over time. The volume, complexity, and effectiveness of the attacks have also intensified. For example, recent statistics maintained by the IT Branch show that the City receives up to 8,000 attempts per month to breach the City's IT security systems through email.

There is a constantly-evolving nature to IT risks, as aggressors try to find new ways to defeat counter measures put in place. Every computer, mobile device, program and employee user account represents a potential risk to the City's IT system. Exhibiting sound governance, and having strong controls in place to manage risk in a structured manner, is the most appropriate and responsible way to manage any risks that exceed the organization's defined risk tolerance level.

3 Audit Objective

The audit objective for this project was to assess the effectiveness of the City's IT risk management process, supporting framework, and policies using the following criteria:

1. Responsibility for risk is defined and operational
2. A formal process is in place to manage IT risks, including identification, assessment, and monitoring
3. The City's IT risk management process is effectively governed

4 Scope and Methodology

Audit Scope

Our focus was on the IT risk management process and related procedures, and did not seek to evaluate the City-wide ERM process. The extent of work related to ERM was to ensure that the IT Risk Management Program aligned with the ERM process approved by Council.

Methodology

In order to achieve our audit objective we:

- Interviewed staff responsible for the IT risk management and City-wide ERM functions
- Reviewed industry best practices related to IT risk management
- Evaluated the design of the IT Risk Management Program for alignment with the ERM process and inclusion of best practices
- Reviewed threat assessment and treatment plans, and compared a sample to the requirements contained within the IT Risk Management Program
- Evaluated overall compliance with industry best practices

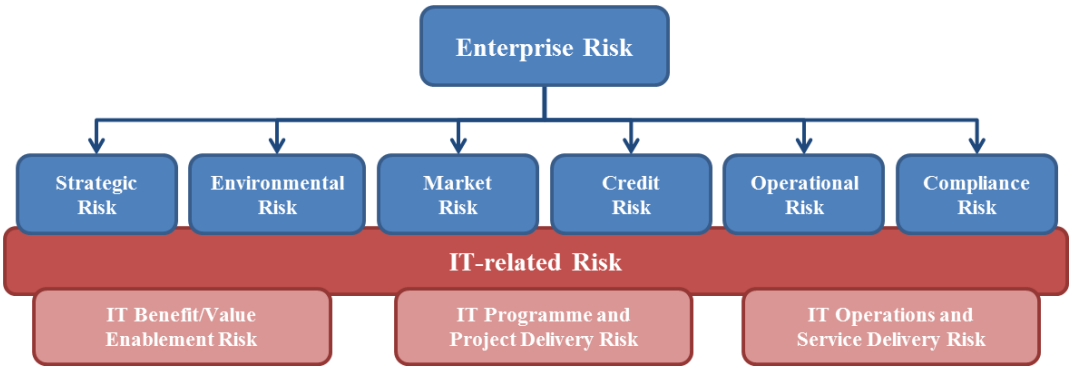
For the purpose of determining best practices as they relate to our audit, we referred to guidance issued by the Information Systems Audit and Control Association (ISACA), which is an internationally-recognized association with a focus on IT governance. These

are reflected in the requirements set out in the following section and are accepted as being the most effective way to achieve the audit objective.

5 Observations and Recommendations

IT risk management is foundational to establishing effective risk and security processes related to the current IT environment, as well as for future changes and expansion. Figure 1 illustrates the position of IT-related risks and how they are woven throughout an organization's operations, such that any issue impacting the IT system would likely have an impact on the City's ability to provide services.

Figure 1 – IT Risk within the Organization[1]



The IT Branch has implemented an IT risk management process to specifically address potential risks that would impact IT systems, They have worked with the Corporate Strategic Planning Branch to ensure that it aligns with the City-wide ERM process.

There are four major steps in the IT risk management process.

1. Risk Governance: to ensure that risk management practices are created, providing context and guidance on the risk management process. A framework or program is created in this step to outline responsibilities and process requirements, including the level of risk tolerance.

[1] ISACA: The Risk IT Framework, 2009

2. Risk Evaluation: to ensure that IT-related risks are identified and assessed in line with the framework created in Step 1.
3. Risk Response: to ensure that any risks determined to be above the acceptable risk tolerance level are addressed in a cost-effective manner.
4. Risk Governance: for regular reporting, to ensure there is senior management awareness and oversight of the entire program.

In order for an IT risk management process to function properly, all the steps listed above must be implemented.

5.1 Criteria 1: Responsibility for Risk

Requirements

We reviewed the IT Risk Management Program, to determine whether:

- IT-risk roles and responsibilities have been established and assigned to staff at appropriate levels; and,
- Senior management has provided direction on the appetite for IT risk and approval of any residual IT risks.

Results

We reviewed the IT Risk Management Program, which lays out the various ownership, roles and responsibilities of staff, as they relate to IT-risk. We found this framework to be appropriately designed and in line with best practices.

Risk management at the City of Edmonton is owned by the City Manager, with accountability then delegated to the Chief Financial Officer and Deputy City Manager, Financial and Corporate Services (CFO). Accountability for IT risk management, as a component of the entire City-wide risk profile, is then further delegated to the IT Branch Manager and Chief Information Officer (CIO). This structure is also in line with best practices.

We discussed the responsibility for IT risk with the Program Manager, IT Security, Risk & Compliance, the CIO and the CFO. Monthly meetings are held to discuss IT risks, emerging issues, and the status of current risk treatment plans.

Risk tolerance for the IT risk management process is set at a slightly more conservative level than that of the ERM process. This is considered to be reasonable based on the pervasiveness of IT risks and their potential impact on City operations.

Conclusion

Overall, we found the IT risk management framework to be appropriately designed and in line with best practices. Responsibility for risk is defined and operational.

5.2 Criteria 2: Assess and Manage IT Risks

Requirements

We reviewed the IT Risk Management Program, IT Risk Strategy, Information Systems Advisory Group Terms of Reference, and had discussions with staff responsible for the IT risk management and City-wide ERM processes. We also reviewed the IT Risk Register and risk treatment plans currently in place. This allowed us to determine whether:

- The IT risk management framework is aligned with the City-wide ERM framework;
- Guidelines have been established that document how IT risks will be identified, evaluated, prioritized and addressed; and,
- The overall risk register, specifically any risk treatment plans in progress, is being monitored on a regular basis.

Results

We found that there is strong alignment between the IT Risk Management Program and the City's ERM process. Guidelines for the identification, evaluation, and prioritization

of IT risks are in place. The Corporate Manager, ERM is a member of the Information Security Advisory Group, and the Program Manager, IT Security, Risk Management & Compliance is a member of the City-wide Corporate Information Management Committee. This provides an opportunity for regular information sharing, and shows that there has been strong cooperation between those responsible for the IT risk management and City-wide ERM processes.

The IT Risk Management Program includes detailed guidance on how IT risks will be identified (such as through risk assessments, post-incident reviews, or business impact evaluations), evaluated (with context and a defined framework to assess likelihood and impact), prioritized (based on the evaluation), and addressed (tailored to the specific risk).

The IT Branch identified and evaluated risks in accordance with the approved program, and has a process in place to monitor risks and the treatment plans that are in place. At a minimum, there are monthly briefings held between the Program Manager, IT Security, Risk Management & Compliance and the CIO to perform this monitoring.

All risks that were determined to be above the acceptable tolerance have treatment plans in place to address the risks.

Conclusion

There is a structured, formal program in place that follows industry best practices to manage IT risks. This includes risk identification, assessment, and monitoring.

5.3 Criteria 3: IT Risk Management Governance

Requirements

We reviewed the IT Risk Management Program and interviewed staff members to determine compliance with the following:

- Senior management is involved in the IT risk process and receives reports on exposures, response measures in place, and material residual risk that is outstanding;
- Management monitoring is in place to ensure that IT risk management is operating as required, and that management has resources in place to be able to properly manage IT risks; and,
- There is a defined escalation and follow-up process in place, in cases where risk treatment is not effective or sufficient resources are not available, and risk exposure is considered to be greater than tolerable.

Results

We noted that although regular opportunities are available, the CIO has not reported on the IT risk management to members of senior management, with the exception of monthly meetings held with the CFO. Engaging senior management, specifically at the Corporate Leadership Team level, and informing them of the IT risks faced by the City, as well as how these risks are being addressed, is fundamental to good IT risk management governance. Informing the Corporate Leadership Team of IT risks allows them to disseminate any relevant information to their staff, to assist in addressing those risks.

We found that management does monitor practices to ensure that risk management is operating as intended. Based on our discussions with the CIO and CFO, adequate resources are currently in place to mitigate IT risks.

An escalation process is defined in the IT Risk Management Program. However, as the program has just been established, there has not been a need to escalate an issue or risk.

Although we were not able to test the effectiveness of that process, it is appropriately designed.

Conclusion

With the exception of keeping the Corporate Leadership Team informed, the IT Branch has implemented governance processes that are in line with best practices.

There could be improvement to program visibility, as the CIO should provide regular reports to the Corporate Leadership Team; however, management would need to consider the arena (in public or in private) as much of the information could be highly sensitive in nature. Reporting IT risks in a public forum would provide information that could be used in a way that increases the risk to the City.

Recommendation 1– IT Risk Reporting to Senior Management
The OCA recommends that the IT Branch Manager and Chief Information Officer provide formal updates to the Corporate Leadership Team on a regular basis, including the City's IT risk exposures, measures in place to address the risks, and any material residual risk outstanding.
Management Response and Action Plan
Accepted **Action Plan:** Information Technology (IT) Branch management agrees with this audit recommendation. Effective at the Corporate Leadership Team (CLT) meeting November 3, 2016 and each quarter-end thereafter, the IT Risk Report will be shared with members of CLT. In addition, exceptions to mitigating extreme or high IT risk to within established tolerance in a risk and time appropriate manner will be escalated to CLT.

Per the established IT Risk Management (ITRM) program, the ITRM team will continue to capture threats and oversee and monitor risk treatment undertakings. The team will also continue to timely report and review risks with the IT Branch Manager and Chief Information Officer and Deputy City Manager and Chief Financial Officer, Financial and Corporate Services.

IT Branch management values the effort the Office of the City Auditor has applied to this review and appreciates the professionalism and competence with which this audit was undertaken.

Planned Implementation Date: November 3, 2016

Responsible Party: IT Branch Manager and Chief Information Officer

6 Conclusions

Based on the work performed, we can conclude that the IT Branch has put together an effective IT risk management process. Specifically:

1. Responsibility for IT risk management has been clearly defined and assigned to staff at an appropriate level.
2. The IT Branch has a structured, formalized program in place to identify, assess and manage IT risk. This program follows industry best practices, and is aligned with the City-wide ERM process.
3. The IT risk management process is well-governed. Sharing of information needs improvement, and our report includes a recommendation for the IT Branch Manager and Chief Information Officer to report to senior management on a regular basis.

When followed and applied, this program should assist in appropriately mitigating the threat of IT-related risks.

We thank the staff and management of the IT Branch and others who assisted us in completing this project.