CITY OF NEWTON

FINANCIAL AUDIT ADVISORY COMMITTEE

RISK ASSESSMENT, MONITORING & COMPLIANCE
SUB-COMMITTEE REPORT

Monday, June 9, 2014

Present: Robert Fox (Chairman), Ald. Fuller, Ald. Danberg, and Gail Deegan

City staff present: David Wilkinson (Comptroller) and Maureen Lemieux (Chief of Staff)

The Risk Assessment, Monitoring & Compliance Sub-committee began a discussion on developing a multi-year plan for overall risk assessment and monitoring. The sub-committee is currently looking at one aspect; cash receipts risk assessment and monitoring. This meeting is focused on gathering ideas to develop additional aspects of a risk assessment program. Over the past few years, the external auditors have provided a comment in its management letters that the City should be thinking more deeply and robustly about risk assessment and monitoring. The external auditors recommended that the City of Newton, like all municipalities, periodically perform a risk assessment to anticipate, identify, analyze and manage the risk of asset misappropriation. The comment from this past year's Management Letter is attached. The external auditors provided a list of questions that they feel should be considered when assessments are conducted in the Management Letter comment. (The topics range from identifying which assets are susceptible to misappropriation to internal control weaknesses and how misappropriation of assets might be concealed.) Notably, the auditor's focus is specifically on asset misappropriation.

In addition, the comment notes that development and implementation of a risk assessment program and a program to ensure that the internal controls are in place should be done by the City's management employees. The sub-committee needs to discuss what needs to be done in terms of risk assessment and who should be doing it. The auditors also recommend that any program that is developed should become part of a formal financial policies and procedures manual.

Ald. Fuller provided copies of a few pages of the PriceWaterhouseCoopers's "A Practical Guide to Risk Assessment: How Principles-Based Risk Assessment Enables Organizations to Take the Right Risks," (attached) originally provided to the Sub-committee by Gail Deegan. The information is geared towards the public sector but should be helpful in generating ideas about a risk assessment program. Of the types of risk assessment, the sub-committee felt that the ones most relevant to the City included compliance, internal audit, financial statement, fraud, security and information technology. The sub-committee also thought that the framework of considering both likelihood and impact in relation to specific objectives of the City was useful.

Comptroller David Wilkinson provided the attached list of six items that he believes reflects risks to the City in priority order. The list includes mis-statement of

financial statements, a material breach of a law, contract or trust, misappropriation of City assets, insufficient budgets to provide desired services, and damage or destruction of a City asset with no funding to replace the asset. The list is limited to things that affect the City financially but could be expanded to include items like information security and compliance.

The sub-committee discussed its role in developing a risk assessment program and how broadly risk assessment should be looked at and whether the focus should just be around financial statement risk, and internal audit risk. For example, data security is a rapidly growing concern for the public and private sector and the sub-committee may want to include security risk when developing a risk assessment program.

It was suggested that it may be appropriate to narrow the focus and develop an approach to address risk assessment in specific areas. The discussion included whether the sub-committee should solely focus on the auditor's comment or use the comment to develop approaches to assess other kinds of risk, as well. The sub-committee needs to develop a framework for prioritization of risk assessment and monitoring. Asset misappropriation is the most obvious risk and the one that gets the most headlines. As the sub-committee is already working on creating a cash receipts policy, the next step would be to review the auditor's questions and choose the next area on which to focus. The sub-committee should also consider how management will implement a formal structured risk assessment.

The discussion also included what risks were associated with the City's movable assets like computers, furniture and office supplies. Currently the City does not have a list of movable assets that have a value of less than $15,000. The sub-committee felt that it might appropriate to include a risk assessment process for misappropriation of movable assets.

It was pointed out that it may be beneficial to consider how trust funds are invested and whether there is a risk that the funds are not getting the optimum return on investments.

There are a number of areas that the sub-committee could focus on like asset misappropriation, lost inventory, return on investment vehicles for trusts, and lost revenue. The sub-committee asked Chief of Staff Maureen Lemieux and Comptroller David Wilkinson to think about what the sub-committee should focus on after cash receipts and to consider if there are departments that the Administration is not satisfied with the level of controls, processes and scrutiny.

Respectfully Submitted

Robert Fox, Chairman

Risk Assessment and Monitoring

Comment

When internal controls are *initially* implemented, they are usually designed to adequately safeguard assets. However, over time, these controls can become ineffective due to changes in technology, operations, etc. In addition, changes in personnel and structure, as well as the addition of new programs and services, can add risks that previously did not exist. As a result, all municipalities must periodically perform a risk assessment to anticipate, identify, analyze and manage the risk of asset misappropriation. Risk assessment (which includes fraud risk assessment), is one element of internal control.

The risk assessment should be performed by management-level employees who have extensive knowledge of the City's operations. Ordinarily, the management-level employees would conduct interviews or lead group discussions with personnel who have knowledge of the City's operations, its environment, and its processes. The risk assessment process should consider the City's vulnerability to misappropriation of assets. It should also address operations that involve heightened levels of risk. When conducting the assessment, the following questions should be considered:

- What assets are susceptible to misappropriation?
- What departments receive cash receipts?
- What departments have movable inventory?
- What operations are the most complex?
- How could assets be stolen?
- Are there any known internal control weaknesses that would allow misappropriation of assets to occur and remain undetected?
- How could potential misappropriation of assets be concealed?
- What prior internal control issues could still continue to be problematic?

Once the areas vulnerable to risks have been identified, a review of the City's systems, procedures, and existing controls related to these areas should be conducted. The City should consider what additional controls (if any) need to be implemented to reduce risk.

After risk has been assessed, periodic monitoring of the identified risk areas must be performed in order to evaluate the controls that have been implemented to mitigate the risks. Since control-related policies and procedures tend to deteriorate over time, the monitoring process ensures that controls are fully operational and effective.

Recommendation

We recommend management develop and implement a risk assessment program to periodically anticipate, identify, analyze, and manage the risk of asset misappropriation. The risk assessment program should be formally documented and become part of the City's financial policies and procedures manual.

We recommend management develop and implement a monitoring program to periodically evaluate the operational effectiveness of internal controls. The monitoring process should be documented in order to facilitate the evaluation of controls and to identify improvements that need to be made.

Management's Response

The Risk Assessment Sub Committee of the Financial Audit Advisory Committee expects to work with management of the City and Newton Public Schools in the study of what steps can be taken to begin development of a more formalized risk assessment and monitoring process.

A practical guide to risk assessment:

How principles-based risk assessment enables organizations to take the right risks

PriceWaterhouseCoopers

http://www.pwc.com/en_us/us/issues/enterprise-risk-management/assets/risk_assessment_guide.pdf

Defining risk assessment , p. 5

Risk assessment is a systematic process for identifying and evaluating events (i.e., possible risks and opportunities) that could affect the achievement of objectives, positively or negatively. Such events can be identified in the external environment (e.g., economic trends, regulatory landscape, and competition) and within an organization's internal environment (e.g., people, process, and infrastructure). When these events intersect with an organization's objectives—or can be predicted to do so—they become risks. Risk is therefore defined as "the possibility that an event will occur and adversely affect the achievement of objectives."

Purpose and process, p. 8

Risk assessment is intended to provide management with a view of events that could impact the achievement of objectives. It is best integrated into existing management processes and should be conducted using a top-down approach that is complemented by a bottom-up assessment process.

Types of risk assessment, p. 9 – 11

• Strategic risk assessment. Evaluation of risks relating to the organization's mission and strategic objectives, typically performed by senior management teams in strategic planning meetings, with varying degrees of formality.

• Operational risk assessment. Evaluation of the risk of loss (including risks to financial performance and condition) resulting from inadequate or failed internal processes, people, and systems, or from external events. In certain industries, regulators have imposed the requirement that companies regularly identify and quantify their exposure to such risks. While responsibility for managing the risk lies with the business, an independent function often acts in an advisory capacity to help assess these risks.

• Compliance risk assessment. Evaluation of risk factors relative to the organization's compliance obligations, considering laws and regulations, policies and procedures, ethics and business conduct standards, and contracts, as well as strategic voluntary standards and best practices to which the organization has committed. This type of assessment is typically performed by the compliance function with input from business areas.

• Internal audit risk assessment. Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives. The assessment considers the impact of risks to shareholder value as a basis to define the audit plan and monitor key risks. This top-down approach enables the coverage of internal audit activities to be driven by issues that directly impact shareholder and customer value, with clear and explicit linkage to strategic drivers for the organization.

•Financial statement risk assessment. Evaluation of risks related to a material misstatement of the organization's financial statements through input from various parties such as the controller, internal audit, and operations. This evaluation, typically performed by the finance function, considers the characteristics of the financial reporting elements (e.g., materiality and susceptibility of the underlying accounts, transactions, or related support to material misstatement) and the effectiveness of the key controls (e.g., likelihood that a control might fail to operate as intended, and the resultant impact).

• Fraud risk assessment. Evaluation of potential instances of fraud that could impact the organization's ethics and compliance standards, business practice requirements, financial reporting integrity, and other objectives. This is typically performed as part of Sarbanes-Oxley compliance or during a broader organization-wide risk assessment, and involves subject matter experts from key business functions where fraud could occur (e.g., procurement, accounting, and sales) as well as forensic specialists.

• Market risk assessment. Evaluation of market movements that could affect the organization's performance or risk exposure, considering interest rate risk, currency risk, option risk, and commodity risk. This is typically performed by market risk specialists.

• Credit risk assessment. Evaluation of the potential that a borrower or counterparty will fail to meet its obligations in accordance with agreed terms. This considers credit risk inherent to the entire portfolio as well as the risk in individual credits or transactions, and is typically performed by credit risk specialists.

• Customer risk assessment. Evaluation of the risk profile of customers that could potentially impact the organization's reputation and fi nancial position. This assessment weighs the customer's intent, creditworthiness, affiliations, and other relevant factors. This is typically performed by account managers, using a common set of criteria and a central repository for the assessment data.

• Supply chain risk assessment. Evaluation of the risks associated with identifying the inputs and logistics needed to support the creation of products and services, including selection and management of suppliers (e.g., up-front due diligence to qualify the supplier, and ongoing quality assurance reviews to assess any changes that could impact the achievement of the organization's business objectives).

•Product risk assessment. Evaluation of the risk factors associated with an organization's product, from design and development through manufacturing, distribution, use, and disposal. This assessment aims to understand not only the revenue or cost impact, but also the impact on the brand, interrelationships with other products, dependency on third parties, and other relevant factors. This type of assessment is typically performed by product management groups.

•Security risk assessment. Evaluation of potential breaches in an organization's physical assets and information protection and security. This considers infrastructure, applications, operations, and people, and is typically performed by an organization's information security function.

•Information technology risk assessment. Evaluation of potential for technology system Failures and the organization's return on information technology investments. This assessment would consider such factors as processing capacity, access control, data protection, and cyber crime. This is typically performed by an organization's information technology risk and governance specialists.

• Project risk assessment. Evaluation of the risk factors associated with the delivery or implementation of a project, considering stakeholders, dependencies, timelines, cost, and other key considerations. This is typically performed by project management teams.

Assessment using likelihood and impact, p. 17

Figure 2. Risks should be assessed considering the likelihood and impact of such risks in relation to specific objectives

Likelihood	Definition	Description	Example *Objective:* Hire staff with appropriate competencies *Event:* Burdensome recruitment procedures limit the organization's ability to attract talent
1	Unlikely	The risk is seen as unlikely to occur within the time horizon contemplated by the objective.	Although **recruitment procedures are burdensome**, talent with appropriate competencies can still largely be attracted and hired.
2	Likely	The risk is seen as likely to occur within the time horizon contemplated by the objective.	**Burdensome recruitment procedures** cause delays and lost opportunities in the hiring of talent with appropriate competencies.
3	Certain/ imminent	The risk is expected to occur within the time horizon contemplated by the objective.	**Burdensome recruitment procedures** cause talent with appropriate competencies to not be attracted or hired.

Impact	Definition	Description	Example
1	Negligible	The risk will not substantively impede the achievement of the objective, causing minimal damage to the organization's reputation.	The extent to which **recruitment procedures are burdensome** will not substantively impede our ability to attract and hire staff with appropriate competencies, causing minimal damage to the organization's reputation.
2	Moderate	The risk will cause some elements of the objective to be delayed or not be achieved, causing potential damage to the organization's reputation.	The extent to which **recruitment procedures are burdensome** will cause delays in our ability to attract and hire staff with appropriate competencies, causing potential damage to the organization's reputation.
3	Critical	The risk will cause the objective to not be achieved, causing damage to the organization's reputation.	The extent to which **recruitment procedures are burdensome** will cause us to be unable to attract and hire staff with appropriate competencies, causing damage to the organization's reputation.

Financial statements will be materially misstated

There will be a material breach of a state/federal/local law; contract; or trust agreement

City assets will be misappropriated and/or misused

Operating and/or capital budgets will be insufficient to provide desired services

One or more City asset , used to provide public services, will be damaged or destroyed

Desired operating budget results ~~are~~ will not be achieved