



CITY OF  
**Tulsa**  
A New Kind of Energy.

# **2012 IT RISK ASSESSMENT**

**As of December 31, 2012**

---

**City of Tulsa Internal Auditing**

**January 2013**

# MEMORANDUM


OFFICE OF THE CITY AUDITOR



---

DATE: January 22, 2013

TO: Mayor Dewey Bartlett  
Councilor Jack Henderson  
Councilor Jeannie Cue  
Councilor David Patrick  
Councilor Blake Ewing  
Councilor Karen Gilbert  
Councilor Byron "Skip" Steele  
Councilor Arianna Moore  
Councilor Phil Lakin, Jr.  
Councilor G. T. Bynum

FROM: Clift Richards, CPA, City Auditor 

SUBJECT: 2012 IT Risk Assessment Internal Audit Report

I am pleased to present the following report of the subject audit. Internal Auditing contracted with Sunera, LLC to co-source execution of the audit. Sunera is a leading provider of risk based consulting services throughout the United States and Canada with considerable experience across a multitude of industries including local, state & federal governments in delivering a broad range of IT advisory and assessment services. The audit was conducted by a joint team of Sunera and City of Tulsa, Internal Auditing.

Suggested actions were presented to City of Tulsa IT management who provided a detailed response to the improvement opportunities discussed in the internal audit report. We would like to express our appreciation to those members of the Information Technology Department who worked with us to make this audit a success. We especially recognize the following who, among others, exhibited a commendable degree of dedication to improvement of City of Tulsa information technology operations: Major Jonathan Brooks, Brett Tabler, Rick Lisenbee and John Robertson.

We welcome questions and comments. Please let us know if you would like additional information.



# 2012 IT RISK ASSESSMENT

AS OF DECEMBER 31, 2012

## City of Tulsa Internal Auditing

Handwritten signature of Ron Maxwell in black ink.

---

Ron Maxwell, CIA, CFE  
Chief Internal Auditor

Handwritten signature of Cliff Richards in black ink.

---

Cliff Richards, CPA  
City Auditor

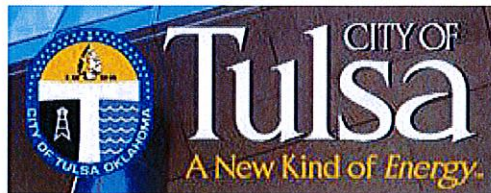
### AUDIT TEAM:

#### **SUNERA, LLC**

Brian Amend, CPA, CIA, CFSA, CCSA, CIDA  
Managing Partner – Texas Practice Sunera  
Terry Quan, Senior Manager Sunera

#### **CITY OF TULSA**

Steve Jackson, CPA Internal Audit Manager  
Lela Walden, CPA



## 2012 IT RISK ASSESSMENT REPORT

DECEMBER 31, 2012

## TABLE OF CONTENTS

|  |    |
|--|----|
| Executive Summary .....  | 2  |
| Internal Audit Report .....  | 3  |
| <i>Introduction</i> .....  | 3  |
| <i>Objectives</i> .....  | 3  |
| <i>Approach</i> .....  | 3  |
| <i>Scope</i> .....   | 4  |
| <i>Procedures</i> .....  | 4  |
| Definition of the IT Processes at Risk (Risk Family and Sub-process) ..... | 4  |
| Risk Ratings for identified Risk Families and Sub-processes .....          | 5  |
| Risk Calculation in RAP .....  | 7  |
| <i>Summary of Observations &amp; Recommendations</i> .....                 | 8  |
| <i>Conclusion</i> .....  | 8  |
| <i>Exhibit A – Detailed Observations</i> .....                             | 9  |
| <i>Exhibit B – Risk Scores and Audit Plan</i> .....                        | 23 |
| <i>Exhibit C – IT Risk Dashboard</i> .....                                 | 24 |

## EXECUTIVE SUMMARY

### **Purpose and Objective**

Sunera conducted a Risk Assessment (the "Risk Assessment") of the Information Technology ("IT") environment in order to identify and document the level of risk associated with the Information Technology processes currently in place at the City of Tulsa. The risks associated with the IT processes will be rated at the qualitative level as Low (L), Medium (M) or High (H). The purpose of the Risk Assessment is to identify auditable areas in a risk-based approach so the City can obtain the greatest value from Internal Audit resources *Summary of Observations and Recommendations*

### **Review Observations**

Sunera made fourteen (14) observations related to the IT environment that had a risk score of high or medium. These fourteen observations are related to fifteen sub-processes. One of the observations pertains to two sub-processes, Security Administration (Access Provisioning, Monitoring & Response), and Reporting & Confidentiality. Six of the observations were rated high risk and eight were rated as medium risk.

### **Recommendations**

Recommendations were prepared by Sunera. It is important to note that in most cases, IT management already had an action plan to address the observations. Sunera recommends formally documenting the action plans and defining a timeline for the corrections to be implemented.

### **Conclusion**

Sunera sincerely appreciates the support and cooperation provided by the City employees throughout the course of this Risk Assessment. Additionally, we acknowledge and commend the team's commitment for continuous improvement of internal controls within the established corporate policies and procedures.

As the recommendations stated in this report are addressed, the standards of fiscal and management discipline, including accountability, effectiveness and efficiency of the processes and controls, as well as the mitigation of risks to the management and employees will be strengthened and improved.

## **INTERNAL AUDIT REPORT**

### **Risk Assessment of the Information Technology Environment**

#### ***Introduction***

Sunera conducted a Risk Assessment of the IT environment currently in place at the City of Tulsa (the "City"). The Risk Assessment was conducted using Sunera's methodology, as well as taking into consideration risk factors as stated by process owners during the interview process. Risk factors, as described in the following sections, are used to determine the likelihood of an inherited information technology risk to materialize. The inclusion of risk factors using Sunera's model results in a client specific assessment rather than a generic evaluation against predefined standards.

For ease of reference, this report is divided into the following sections:

- Objectives
- Approach
- Scope
- Procedures
- Summary of Risk Assessment Observations & Recommendations
- Conclusion

#### ***Objectives***

Sunera performed the IT Risk Assessment in accordance with the City's guidance and in preparation for the Internal Audit Plan for year 2012-13.

The results of the Risk Assessment may be used with other risk assessments to develop a comprehensive enterprise risk management program for the City. In connection with the development of the Risk Assessment, Sunera developed a program and schedule for an ongoing audit of the IT environment.

The Risk Assessment should be reviewed frequently (at least annually) by the City and any third party(ies) the City has engaged to assist with determining if any significant changes have been made to the environment that would require the IT risk management program to be adjusted.

#### ***Approach***

The IT Risk Assessment provides an understanding of the risks associated with the deployment and management of the various hardware, software and network infrastructure technologies. Each technology component has associated risks that need to be identified and evaluated for significance in the specific environment.

Understanding these risks provides management assurance that the infrastructure, procedures and controls in place are directed toward the most significant risks and that risks have been reduced to a known and acceptable level.

Understanding technology risks and their potential impact in the business processes also helps to determine the proper allocation of efforts to perform reviews of IT components. Higher risks should be subject to increased attention to assure the risks are being addressed and that management's measures to reduce the risks are

having the intended mitigating effect. Lower-risk areas should also receive attention since their proper interaction with higher-technology risk assets is needed to provide a technology environment that is reliable, secure and effective. Sunera's approach is risk-based.

The IT Risk Assessment was prepared using Sunera's professional experience as a baseline and then refined by conducting interviews with process owners and reviewing documentation gathered through an information request.

### **Scope**

Sunera assessed the City's IT environment in order to identify and document the current level of risk associated with the significant processes and sub-processes in place to manage and control IT resources.

The Risk Assessment Model utilized by Sunera considers a set of predefined IT processes and sub processes. Based on professional experience, Sunera believes that these set of processes and sub processes cover the critical areas of almost any IT environment.

### **Procedures**

During the IT Risk Assessment, Sunera performed the following steps to evaluate the IT environment from a risk perspective and documented the results.

- Performed interviews with process owners using a predefined set of questions oriented to determine the awareness of the inherited information technology risks and a broad description of the controls in place to address such risks.
- Compared answers obtained from the different process owners.
- Requested samples of documentation to verify some of the answers obtained from process owners.
- From the interviews with process owners identify the impact that risk could have in the specific information technology environment.
- Identified the conditions that can impact (increase or decrease) the likelihood of risks. These conditions are called 'control factors'.
- Used a predefined calculation to determine the residual risk after control factors have been used to determine the likelihood.

The following sections describe the components and risk calculation in the Risk Assessment Model.

#### **Definition of the IT Processes at Risk (Risk Family and Sub-process)**

The Risk Assessment Model was assembled through the definition of seven identified IT risk factors, conducting interviews with IT management and support personnel, and risk ranking the identified IT processes utilizing factors for risk, probability, and impact. The results of this effort include 1) a Risk Appraisal Profile; and 2) an Audit Plan for detailing the residual risks for IT risk factors and sub-processes, facilitating the prioritization and scheduling of IT audits (See Exhibit B).

Sunera started by utilizing a baseline model of seven IT processes based on our professional experience assessing Information Technology environments. The seven IT processes are named Risk Families. These Risk Families are then further subdivided into 25 sub-processes. The use of a predefined base line of well-known IT processes provides a fast track to perform the assessment and produce results.



The IT processes included in the Risk Assessment Model are as follows:

***IT Risk Families***

1. IT Operations
  - a. Problem Management and Event Monitoring
  - b. Segregation of Production and Development Environments
  - c. Backup and Restore Operations
  - d. Disaster Recovery and Business Continuity
  - e. Vendor Management
  - f. Data Center Environment
  
2. Information Security
  - a. Physical Security of Hardware
  - b. Security Administration
  - c. Authentication Controls
  - d. Restrictions on Storage of Sensitive Data
  - e. Anti-Virus Administration
  - f. Intrusion Detection and Prevention
  
3. Systems Development
  - a. Developers Restricted from Production Environment
  - b. Change Management (Methodology and Tools)
  - c. Project Management
  
4. System Software and Database Support
  - a. Patch Management Methodology
  - b. Configuration Standards
  - c. Systems and Database Administration
  
5. Network and Telecommunications Support
  - a. Network Architecture and Design
  - b. Network Management and Monitoring
  
6. IT Strategy / Organization
  - a. Business Alignment / IT Strategy
  - b. Organization and Personnel
  - c. Compliance / Oversight
  
7. IT Applications
  - a. Segregation of Duties
  - b. Reporting and Confidentiality

**Risk Ratings for identified Risk Families and Sub-processes**

The Risk Families and sub-processes are arranged in a risk calculation matrix called Risk Assessment Profile ("RAP"). The RAP is included in a Risk Book, which is part of Sunera's risk assessment tool. The RAP includes risks commonly associated with every sub-process. Questionnaires are used to interview process owners to

capture their opinion regarding risk's likelihood and impact. Answers provided by process owners are used to populate the RAP as risk factors. Risk factors provide a summarized reason behind the assigned likelihood rate.

The purpose of this Risk Assessment is to assess the residual risk for each IT component for the applicable Risk Family once its Likelihood and Impact have been determined. IT sub-processes were assessed as to various risk characteristics related to business criticality, the control factors that could define the likelihood of a threat or vulnerability and the impact that such threats and vulnerabilities will cause if they occur.

#### **Probability ("Likelihood")**

The probability of a threat or vulnerability reflects the Likelihood that situations operating satisfactorily may become unstable or outside the tolerance levels either through internal or external conditions. The following steps were taken to determine the Likelihood of a risk materializing into a threat or vulnerability:

1. A general status of every sub-process in the IT environment was obtained by interviewing process owners.
2. Additional information requests were prepared and presented as the interviews developed.
3. Answers provided and information gathered is summarized and captured in the RAP as Control Factors. Control Factors are statements that indicate the awareness of the controls and the general status of the control environment related to the sub-processes. Please note that Control Factors do not reflect or imply the effectiveness of the stated controls in place. Control Factors affect the determination of the likelihood, either reduction or increase, of a threat or vulnerability.
4. A probability or likelihood of a threat or vulnerability affecting the sub-process was determined based on answers provided and Control Factors.

Likelihood is ranked:

- **H** High, meaning that according to the information gathered, the awareness of the risks **and the stated controls in place**, it is probable that a situation could evolve to become a threat or vulnerability
- **M** Medium, meaning that according to the information gathered, the awareness of the risks **and the stated controls in place**, there is a reasonable probability that a situation could evolve to become a threat or vulnerability
- **L** Low, meaning that according to the information gathered, the awareness of the risks **and the stated controls in place**, there is a remote probability a situation could evolve to become a threat or vulnerability

**Impact**

The impact is an estimation of the potential loss or damage that could occur if a threat or vulnerability materializes (“Impact”). The potential loss or damage is an estimate that considers the immediate loss as well as the recovery costs, not in terms of dollars, but in relative terms ranging from:

- **H** High indicates a loss that could cripple the future viability of the organization.
- **M** Medium impact to the organization. IT services could be affected, but will be restored with minimum or no immediate disruption of critical business.
- **L** Low, nothing or almost no effect in the organization.

**Risk Calculation in RAP**

The Likelihood and Impact of every sub-process are factored to determine the Risk Score. An average is calculated with all Risk Scores for all sub-processes in a risk family. The average Risk Scores are then factored with the inherent risk of every Risk Family to determine the residual risk of the IT Process.

The assessment’s elements of Likelihood and Impact are captured in the RAP and the Residual Risk is then calculated as determined by the Risk Workbook. The following section describes the calculations embedded in the RAP.

**Risk Scoring**

Composite risk is the result of factoring the Likelihood and the Impact determined for every sub-process.

The values assigned to the High (“H”), Medium (“M”) and Low (“L”) Likelihood and Impact elements are as follows, respectively:

|                   |         |         |         |
|-------------------|---------|---------|---------|
| Likelihood values | H = 0.7 | M = 0.4 | L = 0.1 |
| Impact values     | H = 3   | M = 2   | L = 1   |

The calculation of the Risk Scores is performed by multiplying the Likelihood and Impact Metric values. The product value result is assigned High (“H”), Medium (“M”) or Low (“L”) as follows:

|            |         |               |         |
|------------|---------|---------------|---------|
| Risk Score | H > 1.1 | 0.4 < M < 1.1 | L < 0.4 |
|------------|---------|---------------|---------|

For example, if the Likelihood is High (H) and the Impact is Low (L), the Risk Score is calculated as follows:

- High Likelihood - 0.7 x Low Impact -1 = **0.7**
- Risk Score is M ( .04< **0.7** < 1.1)

**Residual Risk Level**

Residual Risk is the average of Sub-Process Risk Scores. The product value result is assigned High (“H”), Medium (“M”) or Low (“L”) as follows:

|               |         |               |         |
|---------------|---------|---------------|---------|
| Residual Risk | H > 2.3 | 1.3 < M < 2.3 | L < 1.3 |
|---------------|---------|---------------|---------|

For Example: 6 Sub-processes with Risk Scores of L, L, H, H, H, and L would result in a Residual Risk of M (e.g.  $(1+1+3+3+3+1)/6 = 2$  or Medium).

**Summary of Observations & Recommendations**

**Risk Assessment Observations**

Sunera made fourteen (14) observations related to the IT environment that had a risk score of high or medium. These fourteen observations are related to fifteen sub-processes. One of the observations pertains to two sub-processes, Security Administration (Access Provisioning, Monitoring & Response), and Reporting & Confidentiality. Six of the observations were rated high risk and eight were rated as medium risk.

**Recommendations**

Recommendations were prepared by Sunera. It is important to note that in most of the cases, IT management already had an action plan to address the observations. Sunera recommends formally documenting the action plans and defining a timeline for the corrections to be implemented.

**Conclusion**

Sunera sincerely appreciates the support and cooperation provided by City employees throughout the course of this Risk Assessment. Additionally, we acknowledge and commend the team’s commitment for continuous improvement of internal controls within the established corporate policies and procedures.

As the recommendations stated in this report are addressed, the standards of fiscal and management discipline, including accountability, effectiveness and efficiency of the processes and controls, as well as the mitigation of risks to the management and employees will be strengthened and improved.

**Exhibit A – Detailed Observations**

**Detailed Observations, Recommendations and Management Responses**

|                              |  |                     |   |                    |             |
|------------------------------|--|---------------------|---|--------------------|-------------|
| <b>No.</b>                   | 1  | <b>Sub-process:</b> | Security Administration (Access Provisioning, Monitoring, & Response) and Reporting & Confidentiality | <b>Risk Score:</b> | <b>High</b> |
| <b>Observation(s):</b>       | The City has not defined role-based system access requirements. User access is defined on a case-by-case basis. Also, access control for many applications is administered by an application development group. Terminating access upon employee termination or transfer is labor intensive, has inherent delays and potential incompleteness. Policies, and possibly processes, do not address employee transfers and access provisioning and termination for contractors.  |                     |   |                    |             |
| <b>Risk(s):</b>              | <p>Transferred or terminated employees or contractors may have access to the City's systems and data.</p> <p>The decentralized access control situation results in access provisioning and termination to be labor intensive, inconsistent and potentially incomplete.</p>   |                     |   |                    |             |
| <b>Recommendation(s):</b>    | <p>Sunera recommends that the City identify systems that contain sensitive data.</p> <p>Develop policy and process for defining and managing access to these systems.</p> <p>With the primary business owner(s), define who should have access, and at what level (admin, edit, view-only) to each of these systems. Compare these required levels of access with actual system access. Change access to address any discrepancies</p> <p>Manage access provisioning and termination to reflect employee and contractor hiring, transfers and terminations to departments using or supporting these systems that contain sensitive data.</p> |                     |   |                    |             |
| <b>Management's Response</b> |  |                     |   |                    |             |
| <b>Comments:</b>             |  |                     |   |                    |             |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.  |                     |   |                    |             |
| <b>Corrective Timeline:</b>  |  |                     |   |                    |             |
| <b>Responsible Party:</b>    |  |                     |   |                    |             |

| No.                                 | 2   | Sub-process: | Intrusion Detection and Prevention | Risk Score: | High |
|-------------------------------------|---|--------------|------------------------------------|-------------|------|
| <b>Observation(s):</b>              | The City has not had a network vulnerability assessment performed either internally or by an outside firm.  |              |                                    |             |      |
| <b>Risk(s):</b>                     | The City's network may be vulnerable to external threats.   |              |                                    |             |      |
| <b>Recommendation(s):</b>           | The City should perform a network vulnerability assessment (VA), and depending on results of the VA, conduct network penetration tests, on an annual basis. |              |                                    |             |      |
| <b><i>Management's Response</i></b> |   |              |                                    |             |      |
| <b>Comments:</b>                    |   |              |                                    |             |      |
| <b>Action Plan(s):</b>              | See Information Technology Department Response at Appendix 1.   |              |                                    |             |      |
| <b>Corrective Timeline:</b>         |   |              |                                    |             |      |
| <b>Responsible Party:</b>           |   |              |                                    |             |      |

| No.                          | 3   | Sub-process: | Developers Restricted from Production Environments | Risk Score: | High |
|------------------------------|---|--------------|--|-------------|------|
| <b>Observation(s):</b>       | Most, if not all, of the older applications are fully supported by one of the application development groups. Full support includes development, access control, administering changes to the development, test and production environments, etc.   |              |  |             |      |
| <b>Risk(s):</b>              | <p>Unauthorized changes are made to production, which may have an adverse impact on the users of that system.</p> <p>Unauthorized access is granted.</p> <p>Highly-skilled system development resources are assigned tasks, such as, access control, that can be performed by less-skilled resources.</p>   |              |  |             |      |
| <b>Recommendation(s):</b>    | <ol style="list-style-type: none"> <li>1. Implement a policy to ensure new systems are designed or have the capability of having its access controlled through Active Directory, or at a minimum, have the capability of having its access controlled through an administration capability that can be delegated to the service desk.</li> <li>2. For systems that contain sensitive data, independently monitor access control changes on a monthly basis.</li> <li>3. Manage access provisioning and termination to reflect employee and contractor hiring, transfers and terminations to departments using or supporting these systems that contain sensitive data.</li> </ol> |              |  |             |      |
| <b>Management's Response</b> |   |              |  |             |      |
| <b>Comments:</b>             |   |              |  |             |      |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.   |              |  |             |      |
| <b>Corrective Timeline:</b>  |   |              |  |             |      |
| <b>Responsible Party:</b>    |   |              |  |             |      |

| No.                          | 4   | Sub-process: | Change Management Methodology and Tools | Risk Score: | High |
|------------------------------|---|--------------|---|-------------|------|
| <b>Observation(s):</b>       | <p>This policy defines the process for enacting changes to Information Technology (IT) production environments (e.g., firewalls, routers, servers, Private Branch Exchanges (PBX), applications, and source code) that can affect programs, systems software, hardware, or any other aspect of the information-processing environment.</p> <p>The adherence to this policy has been inconsistent. Changes have been made where inadequate notification was made to the user community or the user community was adversely impacted by the change.</p> <p>Non-IT departments are allowed to purchase IT solutions and implement outside of the Change Management Policy and then, in some cases, turnover the solution to the IT department for maintenance and support.</p>   |              |   |             |      |
| <b>Risk(s):</b>              | <p>Emergency changes may be implemented without proper authorization, presenting system security, integrity, and availability risks.</p> <p>The unauthorized implementation of developed systems or changes may present a security, availability, or integrity risk to the business.</p> <p>The unauthorized implementation of developed systems or changes may impact the accuracy / validity of transaction processing and/or the validity of data transmissions between systems.</p> <p>Unauthorized software acquisition may not adhere to established policy and conflict with strategic objectives.</p> <p>Unauthorized significant changes may impact system and/or network integrity and availability.</p> <p>Inaccurate or untested data conversions present an integrity risk to transaction processing.</p> <p>Unauthorized infrastructure changes may not follow change management requirements if defined as "Business-as-usual" or "standard" presenting a potential impact to system and data availability, security, and integrity.</p> |              |   |             |      |
| <b>Recommendation(s):</b>    | <ol style="list-style-type: none"> <li>1. Update procurement policies and procedures so that IT hardware and software are not procured without the involvement of the IT department.</li> <li>2. Update change management procedures to ensure consistent application if the change management policy and proper notification to users to minimize the potential adverse impact of the change.</li> </ol>   |              |   |             |      |
| <b>Management's Response</b> |   |              |   |             |      |
| <b>Comments:</b>             |   |              |   |             |      |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.   |              |   |             |      |
| <b>Corrective Timeline:</b>  |   |              |   |             |      |
| <b>Responsible Party:</b>    |   |              |   |             |      |



| No.                                 | 5   | Sub-process: | Configuration Standards | Risk Score: | High |
|-------------------------------------|---|--------------|-------------------------|-------------|------|
| <b>Observation(s):</b>              | <p>The IT control environment lacks critical policy, procedure and guideline documentation. The City relies heavily on the knowledge and dedication of an experienced IT staff.</p> <p>The City does not have formal policies governing configuration standards. It relies heavily on the knowledge and dedication of an experienced IT staff.</p>            |              |                         |             |      |
| <b>Risk(s):</b>                     | <p>Systems may be installed / implemented without proper configuration or adherence to policy, which presents security and integrity risks, in addition to inconsistent / non standardized configurations.</p> <p>The introduction of new systems may present significant security, integrity and availability risks to other systems and/or the network.</p> |              |                         |             |      |
| <b>Recommendation(s):</b>           | <p>IT should develop configuration standards for servers, workstations, wireless access points, web servers and network infrastructure devices.</p>   |              |                         |             |      |
| <b><i>Management's Response</i></b> |   |              |                         |             |      |
| <b>Comments:</b>                    |   |              |                         |             |      |
| <b>Action Plan(s):</b>              | See Information Technology Department Response at Appendix 1.   |              |                         |             |      |
| <b>Corrective Timeline:</b>         |   |              |                         |             |      |
| <b>Responsible Party:</b>           |   |              |                         |             |      |

| No.                          | 6  | Sub-process: | Organization and Personnel | Risk Score: | High |
|------------------------------|--|--------------|----------------------------|-------------|------|
| <b>Observation(s):</b>       | <p>There hasn't been an IT training or travel budget for several years.</p> <p>The IT department has experienced high levels of retirement and turnover. The IT department has a concentration of retirement-eligible employees in a number of critical areas.</p> <p>At the time of this assessment the IT department had 26 vacancies (17.5%).</p> <p>The lack of training budgets adversely affects the ability to attract and retain skilled IT professionals.</p> |              |                            |             |      |
| <b>Risk(s):</b>              | <p>IT department personnel do not develop the knowledge and skills necessary to perform their duties.</p> <p>IT department continues to experience a high turnover rate as employees seek opportunities where they can grow and keep their skills up to date.</p> <p>The IT department continues to find it difficult to attract IT talent in a competitive market.</p>  |              |                            |             |      |
| <b>Recommendation(s):</b>    | <p>Define and gain approval for an ongoing employee development program that provides appropriate training to each IT employee on an annual basis. The cost of such a program is modest when compared to the cost of staff turnover, cost of recruiting and hiring and the cost of providing service with a less knowledgeable and less skilled workforce.</p>   |              |                            |             |      |
| <b>Management's Response</b> |  |              |                            |             |      |
| <b>Comments:</b>             |  |              |                            |             |      |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.  |              |                            |             |      |
| <b>Corrective Timeline:</b>  |  |              |                            |             |      |
| <b>Responsible Party:</b>    |  |              |                            |             |      |

| No.                          | 7  | Sub-process: | Problem Management & Event Monitoring | Risk Score: | Medium |
|------------------------------|--|--------------|---------------------------------------|-------------|--------|
| <b>Observation(s):</b>       | <p>'The IT control environment lacks critical policy, procedure and guideline documentation.</p> <p>The City does not have a formal Problem Management Policy or Procedure. It relies heavily on the knowledge and dedication of an experienced IT staff.</p> <p>A service desk function exists as the point of contact for technical problems. First line support deal with minor issues and complex issues are routed to level two support staff.</p> <p>Incidents reported to the service desk generate a ticket number that can be used to track and report unresolved issues.</p> <p>5 of 6 service desk positions are currently vacant and are manned by contractors with curtailed responsibilities. This results in more incidents being routed to level two support. Also, very difficult to meet 'Serve on First Contact' KPI.</p> |              |                                       |             |        |
| <b>Risk(s):</b>              | <p>Poor problem management may result in the untimely, inefficient and/or ineffective resolution of network, system or user issues.</p> <p>Root cause and resolution steps may not be adequately documented.</p> <p>Incidents may not be timely or effectively addressed, presenting security, integrity and/or availability issues.</p>   |              |                                       |             |        |
| <b>Recommendation(s):</b>    | <ol style="list-style-type: none"> <li>1. Develop and implement Problem Management Policy and Procedure(s).</li> <li>2. Assess and address root causes for high turnover of Service Desk personnel to facilitate hiring and retention of service desk personnel..</li> </ol>   |              |                                       |             |        |
| <b>Management's Response</b> |  |              |                                       |             |        |
| <b>Comments:</b>             |  |              |                                       |             |        |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.  |              |                                       |             |        |
| <b>Corrective Timeline:</b>  |  |              |                                       |             |        |
| <b>Responsible Party:</b>    |  |              |                                       |             |        |

| No.                          | 8   | Sub-process: | Disaster Recovery & Business Continuity | Risk Score: | Medium |
|------------------------------|---|--------------|---|-------------|--------|
| <b>Observation(s):</b>       | <p>The IT control environment lacks critical policy, procedure and guideline documentation. A formal Business Continuity Plan (BRP) does not exist.</p> <p>An annual disaster recovery test is conducted for the systems residing on the main frame. Results are not documented. There is no formal disaster recovery plan for the other systems.</p> <p>Systems have not been classified or prioritized. The City's ability to conduct critical functions after or during a disaster is uncertain.</p>   |              |   |             |        |
| <b>Risk(s):</b>              | <p>Information system, applications, database, and network architecture may not be recoverable in the event of a disaster.</p> <p>Prioritization and criticality of information systems may be inaccurate, impacting the ability to recover from a disaster.</p> <p>Personnel and procedures necessary to recover from a disaster may not be identified or available.</p> <p>The ability to continue business as a result of significant and disruptive events such as pandemics, terrorist attacks, and large scale natural disasters may not be possible.</p> |              |   |             |        |
| <b>Recommendation(s):</b>    | <p>Business and IT Management should perform a business impact analysis and develop a disaster recovery plan and a business continuity plan.</p>  |              |   |             |        |
| <b>Management's Response</b> |   |              |   |             |        |
| <b>Comments:</b>             |   |              |   |             |        |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.   |              |   |             |        |
| <b>Corrective Timeline:</b>  |   |              |   |             |        |
| <b>Responsible Party:</b>    |   |              |   |             |        |

| No.                          | 9   | Sub-process: | Project Management | Risk Score: | Medium |
|------------------------------|---|--------------|--------------------|-------------|--------|
| <b>Observation(s):</b>       | <p>IT projects have high visibility. Their success or failure reflect greatly on the capabilities of the IT department. IT projects require diligent planning and execution to ensure success. Based on vacant positions at the time of this assessment, the PMO is understaffed which raises a concern over the group's ability to manage the projects that are currently active.</p> <p>One of our concerns is related to over commitment of resources to project and non-project activities can adversely impact project schedules. The PMO is not able to assess resource assignments and identify over commitment situations and proactively make adjustments accordingly.</p> |              |                    |             |        |
| <b>Risk(s):</b>              | <p>Projects are not well managed resulting in inefficient use of resources, cost over runs and schedule delays.</p> <p>Less than a stellar track record of managing IT projects can also result in the user community lacking confidence in the IT department. This may result in user departments going outside of the IT department to obtain IT implementation services or may result in user departments delaying decisions to upgrade systems due to prior poor implementation performance.</p>  |              |                    |             |        |
| <b>Recommendation(s):</b>    | <ol style="list-style-type: none"> <li>1. Upgrade the tools used by the IT department to provide better management and communication of IT projects.</li> <li>2. Implement a system that can support all of the work processes within the IT department. This will provide greater visibility as to resource utilization and the availability of resources for projects. By implementing a system that supports all IT work processes, it will be easier to implement needed policies and processes as discussed in this assessment as well as other assessments of the IT department.</li> </ol>   |              |                    |             |        |
| <b>Management's Response</b> |   |              |                    |             |        |
| <b>Comments:</b>             |   |              |                    |             |        |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.   |              |                    |             |        |
| <b>Corrective Timeline:</b>  |   |              |                    |             |        |
| <b>Responsible Party:</b>    |   |              |                    |             |        |

| No.                          | 10  | Sub-process: | Patch Management Methodology | Risk Score: | Medium |
|------------------------------|---|--------------|------------------------------|-------------|--------|
| <b>Observation(s):</b>       | <p>The IT control environment lacks critical policy, procedure and guideline documentation. The City relies heavily on the knowledge and dedication of an experienced IT staff.</p> <p>Desktop Management Group manages 3,000 desktop devices and 850 mobile devices. Group uses Altiris for desktop management. Monitors McAfee updates.</p> <p>Server Services Group is responsible for patch management on the servers. Servers are 1 to 1-1/2 years behind on patch updates. Patches are downloaded automatically but not installed. Go through change management process. Critical security-related patches are installed as soon as possible.</p> |              |                              |             |        |
| <b>Risk(s):</b>              | <p>Software installations may create operation risk, such as security, integrity and availability issues.</p> <p>System software version / patches may not be current, which may present security, integrity and availability issues.</p>   |              |                              |             |        |
| <b>Recommendation(s):</b>    | <p>IT should perform a comprehensive patch management assessment of the computing environment, develop a patch management 'catch-up' plan, and perform updates on all applicable systems.</p>   |              |                              |             |        |
| <b>Management's Response</b> |   |              |                              |             |        |
| <b>Comments:</b>             |   |              |                              |             |        |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.   |              |                              |             |        |
| <b>Corrective Timeline:</b>  |   |              |                              |             |        |
| <b>Responsible Party:</b>    |   |              |                              |             |        |

| No.                          | 11  | Sub-process: | Systems and Database Administration | Risk Score: | Medium |
|------------------------------|---|--------------|-------------------------------------|-------------|--------|
| <b>Observation(s):</b>       | <p>The IT control environment lacks critical policy, procedure and guideline documentation.</p> <p>The City does not have formal policies governing system and database administration. It relies heavily on the knowledge and dedication of an experienced IT staff.</p> <p>System Administration functions are the responsibility of one of the application development groups. The application development groups are aligned based on business function. The responsibilities of the group may vary depending on the vintage of the application and whether the applications was built or bought.</p> <p>One of these application development groups includes the database administration function.</p> |              |                                     |             |        |
| <b>Risk(s):</b>              | <p>The lack of systems administration procedures presents the potential for inconsistent operations, incident handling, and management reporting and management oversight.</p>  |              |                                     |             |        |
| <b>Recommendation(s):</b>    | <ol style="list-style-type: none"> <li>1. Develop and implement a system administration policy and procedure(s).</li> <li>2. Develop and implement a database administration policy and procedure(s).</li> </ol>  |              |                                     |             |        |
| <b>Management's Response</b> |   |              |                                     |             |        |
| <b>Comments:</b>             |   |              |                                     |             |        |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.   |              |                                     |             |        |
| <b>Corrective Timeline:</b>  |   |              |                                     |             |        |
| <b>Responsible Party:</b>    |   |              |                                     |             |        |

| No.                          | 12   | Sub-process: | Network Management & Monitoring | Risk Score: | Medium |
|------------------------------|--|--------------|---------------------------------|-------------|--------|
| <b>Observation(s):</b>       | <p>Change Management Policy - defines the process for enacting changes to Information Technology (IT) production environments (e.g., firewalls, routers, servers, Private Branch Exchanges (PBX), applications, and source code) that can affect programs, systems software, hardware, or any other aspect of the information-processing environment.</p> <ul style="list-style-type: none"> <li>-Network device changes must follow change procedures.</li> <li>-External Vulnerability scans / tests are not performed annually.</li> <li>-Regular Active Directory and VPN User reviews are not performed.</li> <li>-Regular capacity/utilization monitoring is not performed.</li> </ul> |              |                                 |             |        |
| <b>Risk(s):</b>              | <p>Configuration changes may occur and go unnoticed, which may present security, integrity and availability risks to the computing environment.</p> <p>Capacity Management / monitoring practices may not be effective in determining the need to increase bandwidth, address root-causes, or report on usage presenting potential risks to network and system availability.</p>   |              |                                 |             |        |
| <b>Recommendation(s):</b>    | <ol style="list-style-type: none"> <li>1. Refer to recommendations for items 2 and 4.</li> <li>2. Develop and implement a procedure to review Active Directory and VPN User accounts.</li> <li>3. Develop and implement a procedure to monitor capacity and utilization of key network and system resources.</li> </ol>  |              |                                 |             |        |
| <b>Management's Response</b> |  |              |                                 |             |        |
| <b>Comments:</b>             |  |              |                                 |             |        |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.  |              |                                 |             |        |
| <b>Corrective Timeline:</b>  |  |              |                                 |             |        |
| <b>Responsible Party:</b>    |  |              |                                 |             |        |



| No.                          | 13   | Sub-process: | Compliance/Oversight | Risk Score: | Medium |
|------------------------------|--|--------------|----------------------|-------------|--------|
| <b>Observation(s):</b>       | <p>The IT control environment lacks critical policy, procedure and guideline documentation. The City relies heavily on the knowledge and dedication of an experienced IT staff.</p> <p>The Internal Audit Plan includes an annual IT Risk Assessment.</p> <p>A comprehensive review and update of IT controls has not been performed. However, the Internal Audit Department plans to conduct an IT General Controls Audit in 2012-13.</p> <p>Anecdotal evidence indicates that some of the policies and procedures that are in place do not accurately reflect current processes and practices. Many of the existing policies do not have supporting implementing procedures.</p> |              |                      |             |        |
| <b>Risk(s):</b>              | <p>Self-Assessments are not performed to determine if defined controls are operating effectively and/or there is need to update, formalize, and/or define additional controls.</p> <p>Policy and Procedures may not accurately reflect current processes / practices, presenting the potential for compliance deficiencies and the use of inaccurate reference documentation.</p>  |              |                      |             |        |
| <b>Recommendation(s):</b>    | <p>Refer to recommendations to other items in this assessment that pertain to the development and implementation of various policies and procedures.</p>   |              |                      |             |        |
| <b>Management's Response</b> |  |              |                      |             |        |
| <b>Comments:</b>             |  |              |                      |             |        |
| <b>Action Plan(s):</b>       | See Information Technology Department Response at Appendix 1.  |              |                      |             |        |
| <b>Corrective Timeline:</b>  |  |              |                      |             |        |
| <b>Responsible Party:</b>    |  |              |                      |             |        |

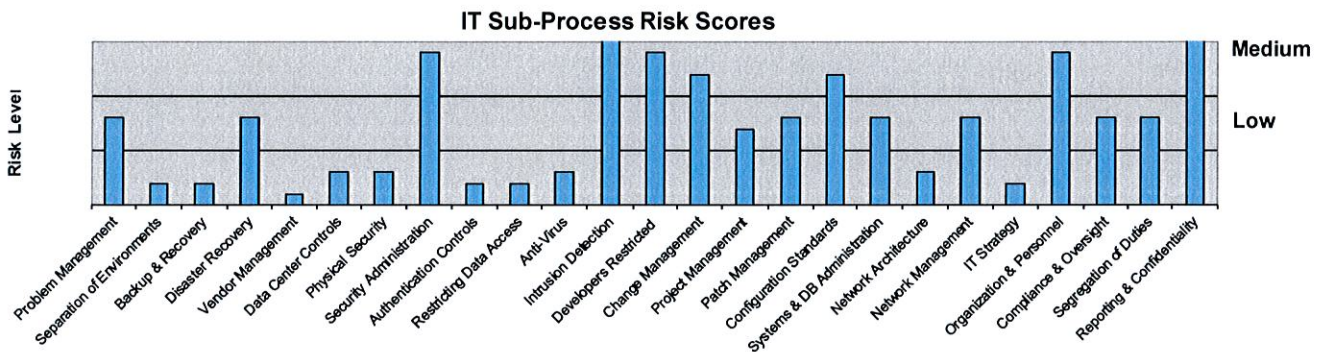
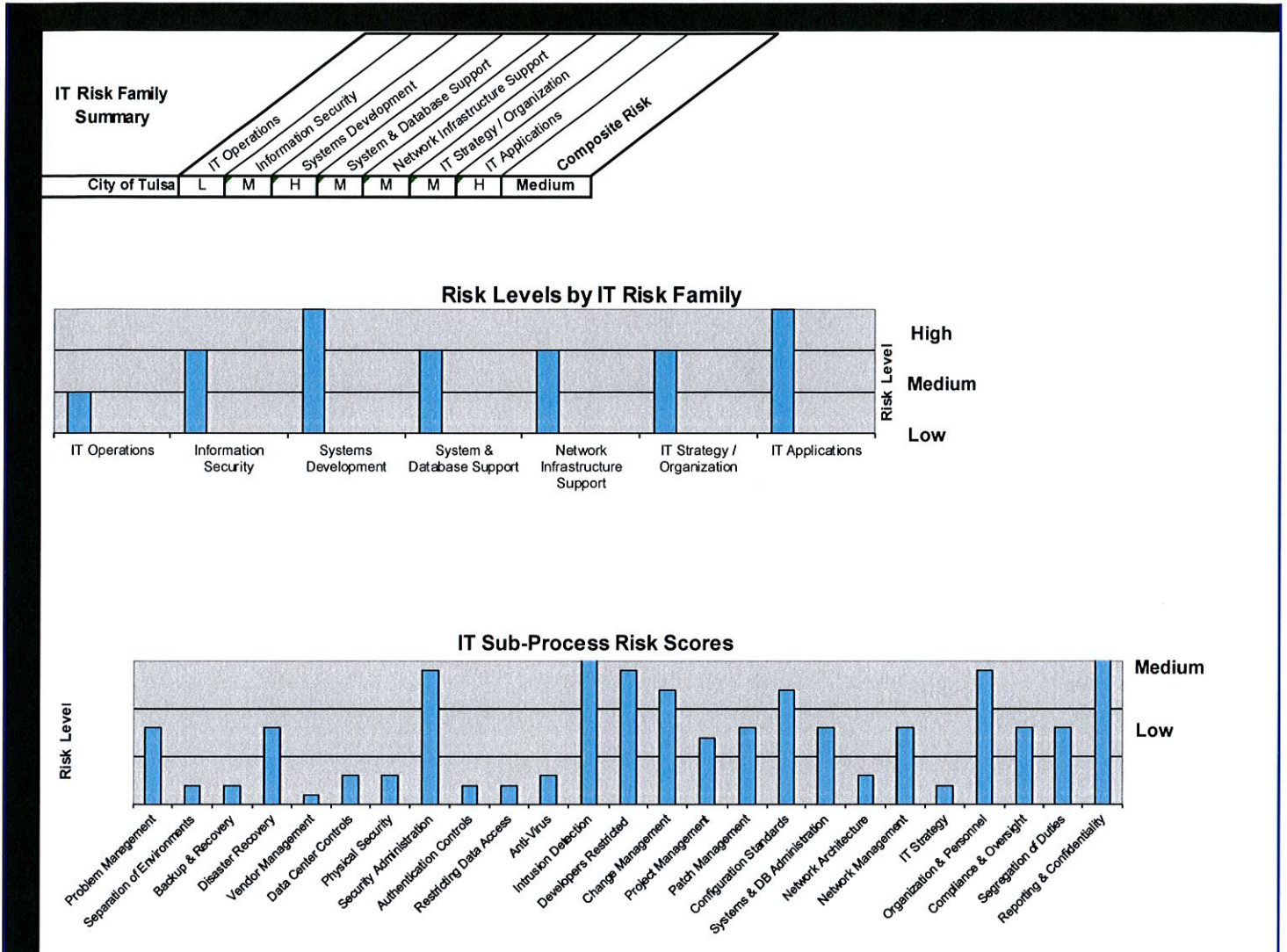
| No.                                 | 14  | Sub-process: | Segregation of Duties | Risk Score: | Medium |
|-------------------------------------|---|--------------|-----------------------|-------------|--------|
| <b>Observation(s):</b>              | <p>Financial system segregation of duties are defined by the City's Finance Department and are manually implemented by the Finance Department and the applications development group that supports the finance systems.</p> <p>Segregation of duties outside of the finance systems is not defined, and therefore not documented.</p> |              |                       |             |        |
| <b>Risk(s):</b>                     | <p>Application controls are not effectively configured to ensure that system users cannot perform conflicting duties, which presents a risk to system and data integrity and security.</p>  |              |                       |             |        |
| <b>Recommendation(s):</b>           | <ol style="list-style-type: none"> <li>1. Business representatives should identify additional segregation of duty requirements.</li> <li>2. The City should develop procedures to manage system access restrictions that support defined segregation of duties requirements.</li> </ol>   |              |                       |             |        |
| <b><i>Management's Response</i></b> |   |              |                       |             |        |
| <b>Comments:</b>                    |   |              |                       |             |        |
| <b>Action Plan(s):</b>              | See Information Technology Department Response at Appendix 1.   |              |                       |             |        |
| <b>Corrective Timeline:</b>         |   |              |                       |             |        |
| <b>Responsible Party:</b>           |   |              |                       |             |        |

### Exhibit B – Risk Scores and Audit Plan

The following table presents the resulting risk scores for each IT sub-process reviewed as part of the IT Risk Assessment. A high-risk score does not indicate that significant problems exist in a process. “High Risk,” as used throughout this report, is defined as a high likelihood of unfavorable events occurring in the process combined with a potentially high negative impact on the related process objectives should an unfavorable event occur.

| Risk Family                             | Residual Risk | Sub- Process   | 2012 Risk Score | 2013 Risk Score |
|---|---------------|--|-----------------|-----------------|
| <b>IT Operations</b>                    | <b>L</b>      | <b>Controls testing should occur at least Annually</b> |                 |                 |
|   |               | Problem Management and Event Monitoring                | Medium          |                 |
|   |               | Segregation of Production and Development Environments | Low             |                 |
|   |               | Backup and Restore Operations                          | Low             |                 |
|   |               | Disaster Recovery and Business Continuity              | Medium          |                 |
|   |               | Vendor Management                                      | Low             |                 |
|   |               | Data Center Environment                                | Low             |                 |
| <b>Information Security</b>             | <b>M</b>      | <b>Controls testing should occur at least Annually</b> |                 |                 |
|   |               | Physical Security of Hardware                          | Low             |                 |
|   |               | Security Administration                                | High            |                 |
|   |               | Authentication Controls                                | Low             |                 |
|   |               | Restrictions on Storage of Sensitive Data              | Low             |                 |
|   |               | Anti-Virus Administration                              | Low             |                 |
|   |               | Intrusion Detection and Prevention                     | High            |                 |
| <b>Systems Development</b>              | <b>H</b>      | <b>Controls testing should occur Quarterly</b>         |                 |                 |
|   |               | Developers Restricted from Production Environment      | High            |                 |
|   |               | Change Management (Methodology and Tools)              | High            |                 |
|   |               | Project Management                                     | Medium          |                 |
| <b>Systems and Database Support</b>     | <b>M</b>      | <b>Controls testing should occur at least Annually</b> |                 |                 |
|   |               | Patch Management Methodology                           | Medium          |                 |
|   |               | Configuration Standards                                | High            |                 |
|   |               | Systems and Database Administration                    | Medium          |                 |
| <b>Network / Infrastructure Support</b> | <b>M</b>      | <b>Controls testing should occur at least Annually</b> |                 |                 |
|   |               | Network Architecture and Design                        | Low             |                 |
|   |               | Network Management and Monitoring                      | Medium          |                 |
| <b>IT Strategy / Organization</b>       | <b>M</b>      | <b>Controls testing should occur at least Annually</b> |                 |                 |
|   |               | Business Alignment / IT Strategy                       | Low             |                 |
|   |               | Organization and Personnel                             | High            |                 |
|   |               | Compliance / Oversight                                 | Medium          |                 |
| <b>IT Applications</b>                  | <b>H</b>      | <b>Controls testing should occur Quarterly</b>         |                 |                 |
|   |               | Segregation of Duties                                  | Medium          |                 |
|   |               | Reporting and Confidentiality                          | High            |                 |

**Exhibit C – IT Risk Dashboard**



**2012 IT RISK ASSESSMENT, BY SUNERA, LLC  
INFORMATION TECHNOLOGY DEPARTMENT RESPONSE  
JANUARY 11, 2013**

# 2012 IT Risk Assessment, by Sunera LLC

## The Information Technology Department Response

Major Jonathan Brooks, Interim Chief Information Officer



## Introduction

The Internal Auditing Department engaged Sunera LLC, a provider of risk based consulting services, to assess the City's Information Technology (IT) environment in order to identify and document the current level of risk associated with the significant processes and sub-processes in place to manage and control IT resources. That work was performed through a series of interviews with senior IT management and staff in the summer of 2012. Their draft report, entitled 2012 IT Risk Assessment, dated November 9, 2012, was submitted to the City for review. In this report the assessment is referred to as *Sunera*.

## Sunera's methodology

Sunera's methodology included:

- Performing interviews with process owners using a predefined set of questions oriented to determine the awareness of the inherited information technology risks and a broad description of the controls in place to address such risks.
- Comparing answers obtained from the different process owners.
- Requesting samples of documentation to verify answers obtained from process owners.
- From the interviews with process owners identifying the impact that risk could have in the specific information technology environment.
- Identifying the conditions that can impact (increase or decrease) the likelihood of risks. Sunera refers to these as 'control factors'.
- Using a predefined calculation to determine the residual risk after control factors have been used to determine the likelihood.

The interviews were guided discussions of the threats and vulnerabilities of IT operations as perceived by the interviewees.

## IT Risk Families

Sunera defines 7 high-level risk factors, called risk families, and categorizes processes and sub-processes within those risk families<sup>1</sup>. Sunera deduced medium or high risk in 15 of these 25 sub-processes in IT and reported on each in their Detailed Observations, noted by italics with their detailed observation number and risk rating.

1. IT Operations
  - *Problem Management and Event Monitoring (7 – Medium)*
  - Segregation of Production and Development Environments
  - Backup and Restore Operations
  - *Disaster Recovery and Business Continuity (8 – Medium)*
  - Vendor Management
  - Data Center Environment

---

<sup>1</sup> Sunera, page 5.

2. Information Security
  - Physical Security of Hardware
  - *Security Administration (1 – High)*
  - Authentication Controls
  - Restrictions on Storage of Sensitive Data
  - Anti-Virus Administration
  - *Intrusion Detection and Prevention (2 – High)*
3. Systems Development
  - *Developers Restricted from Production Environment (3 – High)*
  - *Change Management (Methodology and Tools) (4 – High)*
  - *Project Management (9 – Medium)*
4. System Software and Database Support
  - *Patch Management Methodology (10 – Medium)*
  - *Configuration Standards (5 – High)*
  - *Systems and Database Administration (11 – Medium)*
5. Network and Telecommunications Support
  - Network Architecture and Design
  - *Network Management and Monitoring (12 – Medium)*
6. IT Strategy/Organization
  - Business Alignment/IT Strategy
  - *Organization and Personnel (6 – High)*
  - *Compliance/Oversight (13 – Medium)*
7. IT Applications
  - *Segregation of Duties (14 – Medium)*
  - *Reporting and Confidentiality (1 – High)*

## The risk ratings<sup>2</sup>

- High risk

*According to the information gathered, the awareness of the risks and the stated controls in place, it is probable that a situation could evolve to become a threat or vulnerability*

1. Security Administration
2. Reporting and Confidentiality
3. Intrusion Detection and Prevention
4. Developers Restricted from Production Environment
5. Change Management (Methodology and Tools)
6. Organization and Personnel

- Medium risk

---

<sup>2</sup> Sunera, page 6.



*According to the information gathered, the awareness of the risks and the stated controls in place, there is a reasonable probability that a situation could evolve to become a threat or vulnerability*

7. Problem Management and Event Monitoring
8. Disaster Recovery and Business Continuity
9. Project Management
10. Patch Management Methodology
11. Systems and Database Administration
12. Network Management and Monitoring
13. Compliance/Oversight
14. Segregation of Duties

## **The Information Technology Department's response**

As Sunera acknowledges<sup>3</sup>, the Information Technology Department (ITD) already has action plans to address most of the reported observations. Correcting the conditions enumerated in Sunera's report and effectively managing IT risk is a long-term program requiring a significant commitment of time and resources.

The detailed observations point out IT risks predominantly in four areas of controls:

- Authentication and access
- Identification and classification of sensitive data
- Process definition and enforcement
- Staff development and training.

The Information Technology Department's plans have short- and long-term goals, some of which depend on collaboration with other departments and an infusion of new resources.

### ***Background***

For over a generation the City has developed information systems to serve the needs of all its departments. From the decentralization of IT in the late 1980s until the reconsolidation in 2005 each department could institute its own IT function, and most did. The Police, Fire, Public Works, and other departments had full service IT operations. The much-reduced Information Services Department served the needs of the rest.

The Information Technology Department inherited these different, and often incompatible, systems and has operated them with high reliability and performance. But the complexity of administering these systems continues to reduce ITD's ability to adapt to new technologies and the changing needs of the departments it serves. One area neglected for many years is a formal and rigorous approach to managing IT risk. The IT Risk Assessment has given ITD the benefit of Sunera's experience to prioritize and realign its risk position to better serve our city.

---

<sup>3</sup> Sunera, page 2.

## ***Authentication and access***

Specialized applications for the Police, Fire, Public Works, Parks & Recreation, Development Services, and other departments have relied on the capabilities of each system to authenticate and authorize users. This is, as Sunera observes<sup>4</sup>, a time-consuming, manual process prone to delay and error. User access request forms for these legacy systems use paper forms, and often are not reviewed for transfers and terminations. While this process does present a security risk, other security measures, such as segregation of the network, restricted physical access, and denial of privately owned devices on the trusted network, do provide some security barrier. ITD does not have the resources to retrofit new authentication methods onto many of these legacy systems, even if vendors provided integration with a singular security protocol such as Active Directory Services. ITD is reviewing all legacy systems for replacement, with security risk a consideration in the assignment of priority for replacement.

While these legacy systems remain, ITD will work with the Human Resources Department to establish a process to communicate transfers and terminations immediately to ITD for revocation of access rights. Improved communication with the business owners of these systems will keep individuals' access rights at the appropriate level.

Our plan is to consolidate authorization and authentication services for all systems into Microsoft Active Directory. ITD has begun that process, requiring all new applications use this industry-standard to grant access for users. It is, in part, a process of attrition, where new applications replace the old, reducing the overall complexity of IT and reducing the cost of IT operations. The granting of access to information systems must remain in the hands of the business owners, but ITD is working to create a more efficient process in collaboration with the business owners and the Human Resources Department.

A secondary issue pertaining to this and other focus areas of the report is the segregation of duties between operational and administrative roles. This is, at least, a requirement in principle<sup>5</sup> and in many countries a regulatory requirement for financial services and is defined for the IT financial systems. The operation of this segregation of duties is documented but manual. A new financial system, now under study, will remedy these shortcomings.

Sunera recommends segregation of duties in other areas, such as application development<sup>6</sup>. The segregation of duties is a recommendation for several processes to ensure oversight to changes to systems. ITD is reviewing its change management, patch management, deployment, and configuration control processes to incorporate segregation of duties. The revised System Development Life Cycle (SDLC) is an example of such an improvement. Expanding the existing release management process to include all applications, including revisions to network-related equipment is under consideration.

---

<sup>4</sup> Sunera, page 9.

<sup>5</sup> Basle Committee on Banking Supervision, *Framework for Internal Control Systems in Banking Organizations*, 1998. Principle 6, page 17.

<sup>6</sup> Sunera, page 11, page 20.

## ***Identification and classification of sensitive data***

Recent events, occurring between the end of the Sunera assessment and the submission of their draft report, have raised the priority of this long-standing issue. The City produces an enormous volume and variety of data, and with so many disparate systems the task of analyzing and classifying all data has been beyond ITD's capability. With the introduction of data warehousing technology there is a long-term plan to classify data within that platform and classify all new data added to it. ITD has hired a data architect and is allocating resources to progress on that front.

Data classification by itself is of limited use, and even that responsibility extends beyond ITD to the system business owners to correctly assess the sensitivity of data elements. For ITD, there must be automated rules to enforce and monitor the location of, use of, and access to, sensitive information. This initiative began with the redesign of the City's connection to the Internet and the data accessible through it. The combination of a centralized data warehouse, a business intelligence interface for users, and strict enforcement of business, legal, and regulatory compliance will reduce the risk of unauthorized access to sensitive data.

There is a link between data classification and the business processes supported by that data. Data classification, as ITD has learned, can avoid many security issues, but not without also integration with IT and business operations. That effort will require modifications to most existing IT processes and incorporation into all new ones. Several Sunera<sup>7</sup> recommendations revolve around the relationship between data and process; ITD cannot correct the risks of one without addressing the risks to the other. ITD is taking a holistic approach as resources allow. The redesign of the DMZ, which identifies and separates sensitive data from publicly accessible resources, is an example of progress in this area.

## ***Process definition and enforcement***

IT operations are a set of processes. Sunera correctly observes the Information Technology Department's process definition and control are inadequate for its mission. ITD has made progress in establishing defined, optimized processes in all divisions of the department to increase performance, reduce cost, and maintain consistency through the inevitable changes in staff and technology. Sunera's recommendations on process improvement are in line with ITD's plans.

ITD has instituted processes for change, incident, problem, and patch management, and also for the purchasing and deployment of new equipment and software. These are in various stages of maturity, and there is a new emphasis on continuous process improvement. Sunera's report points out shortcomings of several IT processes<sup>8</sup> and the department has taken those up. The Information Technology Infrastructure Library (ITIL) provides a framework of best practices for defining and implementing service-supporting processes. COBIT provides a framework for the governance of IT and IT security. The Information Technology Department uses both to develop

---

<sup>7</sup> Sunera, page 9,

<sup>8</sup> Sunera, pages 9, 11, 12, 25, 26, 17, 18, 19, 20, 21, 22.

and improve its services and performance metrics. The Department will use COBIT also to improve its awareness and management of IT risk to the enterprise.

A new entity within ITD, the Information Technology Security Board (ITSB), which includes senior ITD management and representatives of the Management Review Office (MRO) and the City Security Department, has begun to establish governance, compliance, and risk policies and controls over information security. New evolutions of incident and problem management already have improved ITD's ability to reduce the cost and frequency of security events.

The ITSB has taken governance over all IT risk, security, and compliance issues. It has established procedures through which a third-party security firm performs PCI compliance testing against the City's IT infrastructure<sup>9</sup>, and a consulting firm to assist with information security and compliance issues, including additional vulnerability and penetration testing. The success of that effort depends upon ITD's ability to correctly, completely identify and manage the required sensitive data governed by PCI, HIPAA, and other compliance obligations, and correctly supporting the management of that data through robust business and IT processes.

The Information Technology Department is creating a new Disaster Recovery/Business Continuity site at the Citiplex towers at 81<sup>st</sup> Street and South Lewis, which will reduce the risk of disruptions to the City's information services to the departments<sup>10</sup>. ITD has adopted as the same framework as the Department of Homeland Security for its disaster recovery planning<sup>11</sup>.

### ***Staff development and training***

Sunera correctly states the Information Technology Department has not had a budget for training in ten years<sup>12</sup>, yet no other group within the City experiences such continuous, rapid, and radical change. An under-trained staff threatens our ability to transition from older to newer technologies, and as our aging staff retires, taking with them critical organizational knowledge, our inability to offer staff development and training increase the difficulty in recruiting and retaining the highly trained employees the City will need.

The best processes still require knowledgeable and competent staff to execute them. The City will require even better trained and more highly skilled employees as the pace of technological change continues. With new processes, and a program of continuous process improvement, the need for awareness and training in service management and the various supporting processes is greater than ever, and cannot be achieved without additional resources.

---

<sup>9</sup> Sunera, page 10.

<sup>10</sup> Sunera, page 16.

<sup>11</sup> National Fire Protection Association Publication (NFPA) 1600, *Standard on Disaster Recovery/Emergency Management and Business Continuity Programs*, 2010

<sup>12</sup> Sunera, page 14.

***Conclusion***

The Sunera IT Risk Assessment is valuable for its affirmation of issues known to the Information Technology Department for many years. The department has programs underway to correct some of the reported conditions, and is making further plans to correct all.

The Sunera report and recent events has forced an acknowledgement of the resources necessary to complete the recommended actions. The Information Technology Department's current resources constrain it from implementing these recommendations wholesale or quickly. In consultation with the Administration and business units, ITD will incorporate all Sunera's recommendations into its IT Strategic Plan.

## **DISTRIBUTION LIST**

|                                     |
|-------------------------------------|
| Mayor                               |
| Councilor, District 1               |
| Councilor, District 2               |
| Councilor, District 3               |
| Councilor, District 4               |
| Councilor, District 5               |
| Councilor, District 6               |
| Councilor, District 7               |
| Councilor, District 8               |
| Councilor, District 9               |
| City Auditor                        |
| Mayor's Chief of Staff              |
| City Manager                        |
| Chief Technology Officer            |
| Press Secretary                     |
| MRO Director                        |
| Council Administrator               |
| Council Secretary                   |
| Finance Director                    |
| Sr. Admin. Services Officer         |
| Director of Operations & Support IT |
| Director of Applications – IT       |
| External Auditor                    |
| Mayor's Audit Committee             |
| Internal Audit Staff                |