INFORMATION TECHNOLOGY RISK ASSESSMENT
COBIT Processes PO2, AI3, & DS12

City of Tulsa Internal Auditing

February 2013

MEMORANDUM

OFFICE OF THE CITY AUDITOR

DATE: February 28, 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 Information Technology Risk Assessment
COBIT Processes PO2, AI3, & DS12

Enclosed is the report of the subject audit. 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.

This audit was a companion project to the 2012 IT Risk Assessment report issued in January 2013. Execution of the audit was co-sourced by Internal Auditing with Sunera, LLC. Sunera is a leading provider of risk-based consulting services with considerable experience across a multitude of industries including local, state & federal governments. The audit was conducted by a joint team of Sunera and City of Tulsa, Internal Auditing.

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 exhibited 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.

INFORMATION TECHNOLOGY RISK ASSESSMENT

COBIT Processes PO2, AI3, & DS12

City of Tulsa Internal Auditing

Ron Maxwell

Ron Maxwell, CIA, CFE
Chief Internal Auditor

Clift Richards

Clift 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

SUNERA®

CITY OF Tulsa
A New Kind of Energy™

INTERNAL AUDIT REPORT

COVERING

INFORMATION TECHNOLOGY RISK ASSESSMENT

COBIT PROCESSES PO2, AI3, & DS12

NOVEMBER 8, 2012

EXECUTIVE SUMMARY

AUDIT AREA

Audit of the following COBIT (Control Objectives for Information and related Technology) processes:

- PO2 – Define the Information Architecture
- AI3 – Acquire and Maintain Technology Infrastructure
- DS12 – Manage the Physical Environment

BACKGROUND

During July & August 2012, Sunera performed an audit of The City of Tulsa's ("The City's") Information Technology (IT) Department's control environment based on control objectives defined by management and COBIT. The audit was conducted to help ensure the accuracy, completeness, and integrity of key data collected, generated, and maintained as part of The City's IT processes and controls. During the audit, we identified certain areas within the IT environment that require improvement. These areas are summarized in the following Audit Evaluation section.

AUDIT GOAL

Sunera's goal for the audit of the above stated COBIT processes was to determine whether their respective control objectives were being achieved as of 9/30/12.

AUDIT EVALUATION

The following table is a summary of the 3 processes and their objective conclusions that were reviewed, the result of which warrants the review evaluation category as determined by Sunera. Professional judgment was used to determine whether each objective was met, met with recommendations, or not met.

		Objective Conclusion			
Objective	**Description**	**Met**	**Met WR**	**Not Met**	**Report Page**
P02 - Define the Information Architecture					
	PO2.1 Enterprise Information Architecture Model		X		3
	PO2.2 Enterprise Data Dictionary and Data Syntax Rules			X	3
	PO2.3 Data Classification Scheme			X	4
	PO2.4 Integrity Management			X	5
AI3 - Acquire and Maintain Technology Infrastructure					
	AI3.1 Technological Infrastructure Acquisition Plan			X	6
	AI3.2 Infrastructure Resource Protection and Availability			X	6
	AI3.3 Infrastructure Maintenance	X			7
	AI3.4 Feasibility Test Environment			X	7
DS12 Manage the Physical Environment					

		Objective Conclusion			
Objective	**Description**	**Met**	**Met WR**	**Not Met**	**Report Page**
	DS12.1 Site Selection and Layout	X			8
	DS12.2 Physical Security Measures	X			8
	DS12.3 Physical Access	X			8
	DS12.4 Protection Against Environment Factors	X			9
	DS12.5 Physical facilities Management	X			9
Objective Conclusion Summary	Total by Objective Conclusion (of the 13 Objectives Reviewed)	6	1	6	
	% by Objective Conclusion (of the 13 Objectives Reviewed)	46%	8%	46%	

ACCOUNTABLE MANAGERS

Tom Golliver, CIO
Brett Tabler, Director, IT Information Services
Rick Lisenbee, Director, IT Operations & Support

SUMMARY OF MAJOR FINDINGS

The City's IT Department has certain deficiencies, relative to the COBIT processes and controls reviewed, that require immediate attention and remediation.

Management of the audit area, as evidenced by their response in the Summary of Recommendations and Responses, is in agreement with the audit findings and has outlined plans for implementation.

ADMINISTRATION

Audit Report and Summary of Recommendations and Responses: See enclosed.

Distribution copies to: Clift Richards, City Auditor
Ron Maxwell, Chief Internal Auditor
Steve Jackson, Internal Audit Manager
Jonathan Brooks, Interim CIO
Brett Tabler, Director, IT Information Services
Rick Lisenbee, Director, IT Operations & Support

PROCESS PO2: DEFINE THE INFORMATION ARCHITECHTURE

Control Objective PO2.1 - Enterprise Information Architecture Model
Establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT plans as described in PO1. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure.

Conclusion: Objective Met With Recommendations

Observations: A Data Architect was hired in August 2011. Recently, the Data Architect developed a current state application architecture. The version of this document provided for this audit was dated April 2012. The application architecture model has yet to be used in the IT planning process to determine if the model has any effect on the planning process.

Risks: If the City's application architecture model is not used in the IT planning process, then:

1. The City may decide to acquire or develop a new system that duplicates functionality and data of an existing system. This will result in the additional cost of deploying and managing a redundant system and the cost of managing redundant data.
2. A new system may be deployed without the retirement of redundant legacy systems. This will result in the additional costs of supporting redundant systems and managing redundant data.
3. A new system may be deployed without the appropriate integration with existing systems. This will result in additional costs of manual processes to share data between systems or to manually synchronize systems.

Recommendations: Continue with plans to convert the application architecture to database format to support greater uses of the information. Utilize the current state application architecture to support future analysis and decisions to optimize the creation, use and sharing of information by the business.

Management Response:

See Information Technology Department Response at Appendix 1.

Control Objective PO2.2 – Enterprise Data Dictionary and Data Syntax Rules
Maintain an enterprise data dictionary that incorporates the organization's data syntax rules. This dictionary should enable the sharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business users, and prevent incompatible data elements from being created.

Conclusion: Objective Not Met

Observations: The City does not have an enterprise data dictionary. The development of an enterprise data dictionary is a future goal of the Data Architect. The data dictionaries that do exist are maintained on an application or application interface level.

Risks: Without an enterprise data dictionary, the City:

1. May miss opportunities to share data between systems and miss the opportunity of eliminating the cost of managing redundant data.
2. May misunderstand or misinterpret data in their systems. This may result in the misuse of data.
3. Will have difficulty in replacing the knowledge of IT personnel that leave the IT department.

Recommendations:

1. Compile existing data dictionaries from application design documentation and system interface documentation to form the initial enterprise data dictionary.
2. Update the enterprise data dictionary to incorporate the results of the data classification effort per recommendations pertaining to control objective PO 2.3...

Management Response:

See Information Technology Department Response at Appendix 1.

Control Objective PO2.3 – Data Classification Scheme

Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.

Conclusion: Objective Not Met

Observations: Data is not classified at the City. The City has not developed a classification scheme.

Risks: Without a data classification scheme, the City:

1. May not be providing the appropriate level of security and protection to sensitive and critical data.
2. May incur unnecessary cost of applying a high level of security and protection to all data.
3. May be destroying data prematurely or retaining data longer than required or necessary. Destroying data prematurely or retaining data longer than required or necessary have cost and legal ramifications.

Recommendations:

1. Develop a classification scheme.
2. Classify the City's data per the classification scheme.

Management Response:

See Information Technology Department Response at Appendix 1.

Control Objective PO2.4 – Integrity Management
Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.

Conclusion: Objective Not Met

Observations: The City's IT control environment lacks critical policy, procedure and guideline documentation. The City relies heavily on the knowledge and dedication of an experienced IT staff.

The City lacks the following critical policies relevant to this control objective:
- System Access Provisioning and Monitoring Policy
- Data Classification Policy
- Information Security Policy
- Policy that restricts developer access to production environments
- Policy Governing System and Database Administration

Risks:

1. Unauthorized access to systems and data presents a significant security, integrity, and availability risk to the system and/or data.
2. Unauthorized activity may go unnoticed presenting network, system and/or data security and integrity risks.
3. Unclassified or misclassified data may not be backed up and/or retained appropriately, presenting potential operational, financial, and legal risks.
4. Unauthorized system changes may impact the security, integrity, and availability or production systems.
5. The lack of systems administration and database administration procedures presents the potential for inconsistent operations, incident handling, and management reporting and management oversight.

Recommendations:
1. Develop a system access provisioning and monitoring policy.
2. Develop an information security policy.
3. Develop a policy that restricts developer access to production environments.
4. Develop a policy to govern system and database administration.

Management Response:

See Information Technology Department Response at Appendix 1.

PROCESS AI3: ACQUIRE AND MAINTAIN TECHNOLOGY INFRASTRUCTURE

Control Objective AI3.1 – Technological Infrastructure Acquisition Plan
Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organization's technology direction.

Conclusion: Objective Not Met

Observations: The City has compiled a formal set of information technology standards. The version provided for this audit was dated August 29, 2011. However, this document did not include standards for the technological infrastructure.

Risks: If the City does not establish technological infrastructure standards, then it:

1. May acquire and install hardware and/or software that are not compatible with the City's infrastructure.
2. May acquire and install hardware and/or software that are not consistent with the City's intended technology direction.

Recommendations: Update the City's information technology standards to include technology infrastructure.

Management Response:

See Information Technology Department Response at Appendix 1.

Control Objective AI3.2 – Infrastructure Resource Protection and Availability
Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.

Conclusion: Objective Not Met

Observations: The City's IT control environment lacks critical policy, procedure and guideline documentation. The City relies heavily on the knowledge and dedication of an experienced IT staff. The City's IT department does control changes to the infrastructure through its change management process. However, the City's IT department does not have documented policies, procedures or guidelines for capacity management and monitoring.

Risks:

1. 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.

Recommendations: Develop and implement a procedure to monitor capacity and utilization of key network and system resources.

Management Response:

See Information Technology Department Response at Appendix 1.

Control Objective AI3.3 – Infrastructure Maintenance
Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organization's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements.

Conclusion: Objective Met

Observations: Based upon work performed, Sunera feels this objective is being satisfactorily met due to infrastructure changes being subject to the City's IT Change Management Process Policy. The Policy requires review of change requests by the Change Advisory Board which consists of the City's IT Department's Senior Management team. The Change Advisory Board meets on a weekly basis.

Control Objective AI3.4 – Feasibility Test Environment
Establish development and test environments to support effective and efficient feasibility and integration testing of infrastructure components.

Conclusion: Objective Not Met

Observations: The City does not have development and test environments to support effective and efficient feasibility and integration testing of infrastructure components.

Risks:

1. Changes to the production environment may present security, integrity and availability risks to the computing environment.

Recommendations: The City should establish technology infrastructure development and test environments.

Management Response:

See Information Technology Department Response at Appendix 1.

PROCESS DS12: MANAGE THE PHYSICAL ENVIRONMENT

Control Objective DS12.1 – Site Selection and Layout
Define and select the physical sites for IT equipment to support the technology strategy linked to the business strategy. The selection and design of the layout of a site should take into account the risk associated with natural and man-made disasters, while considering relevant laws and regulations, such as occupational health and safety regulations.

Conclusion: Objective Met

Observation: Based upon work performed, Sunera feels this objective is being satisfactorily met due to the location and layout of the City's data center appears to support the business needs of the city and appears to take into account risks associated with natural and man-made disasters.

Control Objective DS12.2 – Physical Security Measures
Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.

Conclusion: Objective Met

Observations: Based upon work performed, Sunera feels this objective is being satisfactorily met due to the following physical security controls being in place at the City's Data Center:

- Data center housed in a secure facility
- Camera with video feed for remote viewing
- Guards located at all entrances to the building. Guards verify proper identification prior to granting access to the building.
- Card key required to access Data center
- Alarm system for the data center
- Server enclosures restrict access to authorized IT personnel.

Control Objective DS12.3 – Physical Access
Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.

Conclusion: Objective Met

Observations: Based upon work performed, Sunera feels this objective is being satisfactorily met due to data center personnel access the data center via card key and all other City employees, contractors, vendors, visitors and other third parties are required to sign in prior to entering the data center.

Control Objective DS12.4 – Protection Against Environmental Factors
Design and implement measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.

Conclusion: Objective Met

Observations: Based upon work performed, Sunera feels this objective is being satisfactorily met due to the following Environmental Controls existing at the Data Center:

- Fire / Heat / Smoke / Humidity Monitoring
- Dry pipe sprinklers, two stage actuation.
- Backup chilled water
- Raised Floor

Control Objective DS12.5 – Physical Facilities Management
Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.

Conclusion: Objective Met

Observations: Based upon work performed, Sunera feels this objective is being satisfactorily met due to the following physical facility controls existing at the Data Center:

- UPS Battery (130 min capacity) & Backup Generator
- Two separate electrical feeds from power company (AEP)
- Raised Floor

APPENDIX 1

INTERNAL AUDIT REPORT COVERING
INFORMATION TECHNOLOGY RISK ASSESSMENT,
COBIT PROCESSES PO2, AI3, & DS12

INFORMATION TECHNOLOGY DEPARTMENT RESPONSE
February 11, 2013

Internal Audit Report covering Information Technology Risk Assessment, COBIT Processes PO2, AI3, & DS12

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. Their goal was to evaluate the Information Technology Department's (ITD) capabilities relative to specific control objectives defined by the Information Security and Control Association (ISACA) in their *Control Objectives for Information and Related Technology* (COBIT) framework.

The Information Technology Department welcomed the opportunity to participate in this effort and now is pleased to offer its response to the audit report. In general, we agree with the results as presented by the Internal Auditing Department and Sunera. Differences we may have we describe in the details of this report.

ITD recognizes we live in a process-driven world, and most organizations of all types can improve their performance by instituting appropriate, repeatable processes. To ensure such processes deliver the expected value, many organizations turn to a system of internal controls, including COBIT, which define control objectives for a successful implementation. Achieving optimal value from a process environment is largely a function of organizational maturity and commitment to improvement. ITD is relatively new to establishing formal processes and operates at a low maturity for most processes. Definitions for the stages of maturity in COBIT 5 are listed in Appendix A.

The Information Technology Department has made improvements since the audit, which are listed in the detailed response. The continued partnership with Internal Auditing will provide the City with a managed cycle of improvement and assurance of information technology.

The Sunera methodology

Sunera interviewed members of the ITD staff, focusing on the IT infrastructure, in July and August of 2012.

The COBIT version used by Sunera was 4.1, released in May of 2007. Sunera performed this audit concurrently with a more general IT Risk Assessment. Sunera selected 3 COBIT 4.1 processes, one from 3 of the 4 process groups, and used those to measure the department's performance:

- PO2, *Define the Information Architecture*
- AI3, *Acquire and Maintain Technology Infrastructure*
- DS12, *Manage the Physical Environment*

The process groups in COBIT 4.1 are Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME).

Each COBIT process includes multiple control objectives with which to measure how well an organization performs the subject function. Table 1 lists all control objectives for the audited processes. Sunera used the interview with IT staff and their own extensive experience to evaluate

ITD performance. Sunera did not evaluate or present any assessment of ITD’s maturity level in the COBIT process implementation.

Table 1. Sunera Audit Summary Conclusions

		Objective Conclusion			
Objective	**Control Objectives**	**Met**	**Met WR**	**Not Met**	**Report Page**
PO2 – Define the Information Architecture					
	PO2.1 Enterprise Information Architecture Model		X		3
	PO2.2 Enterprise Data Dictionary and Data Syntax Rules			X	3
	PO2.3 Data Classification Scheme			X	4
	PO2.4 Integrity Management			X	5
AI3 – Acquire and Maintain Technology Infrastructure					
	AI3.1 Technological Infrastructure Acquisition Plan			X	6
	AI3.2 Infrastructure Resource Protection and Availability			X	6
	AI3.3 Infrastructure Maintenance	X			7
	AI3.4 Feasibility Test Environment			X	7
DS12 – Manage the Physical Environment					
	DS12.1 Site Selection and Layout	X			8
	DS12.2 Physical Security Measures	X			8
	DS12.3 Physical Access	X			8
	DS12.4 Protection Against Environmental Factors	X			9
	DS12.5 Physical Facilities Management	X			9

IT response methodology

ITD supports using COBIT, and is planning to use the latest version, COBIT 5, released in early 2012, to implement internal controls over its services. There are significant differences between versions 4.1 and 5. A full discussion of those differences is out of scope for this document, but where differences are relevant we will describe them. Our response will be in terms of COBIT 5 rather than the now outdated version 4.1. Table 2 shows how the control objectives (CO) of version 4.1 map into the equivalent management practices in version 5.

The 4 COBIT 4.1 process groups become 5 in COBIT 5:

- Align, Plan, & Organize (APO)
- Build, Acquire, & Implement (BAI)
- Deliver, Service, & Support (DSS)
- Evaluate, Direct, & Monitor (EDM)
- Monitor, Evaluate, & Assess (MEA).

All COBIT processes are interdependent, with inputs from and outputs to other processes. An example of this is Table 2, which shows all the inputs and outputs for the COBIT 4.1 process PO2, *Define the Information Architecture*. This makes a difference in how ITD approaches its response to the audit and its plan for COBIT implementation. A process may not be valid until defined by its inputs. ITD may defer implementing an audit recommendation until the control objectives providing the required inputs are in place.

Sunera found ITD had met all control objectives for COBIT 4.1 process *DS12, Manage the Physical Environment*. While ITD strives to improve all processes, and COBIT 5 has a little different perspective, we omit any discussion of physical security to remain within the scope of this response.

Table 2. Mapping COBIT 4.1 Control Objectives to COBIT 5

COBIT 4.1 Control Objective		**COBIT 5 Management Practice**	
PO2.1	Enterprise Information Architecture Model	APO03.02	Define Reference Architecture
PO2.2	Enterprise Data Dictionary & Data Syntax Rules	APO03.02	Define Reference Architecture
PO2.3	Data Classification Scheme	APO03.02	Define Reference Architecture
PO2.4	Integrity Management	APO01.06	Define Information (data) and System Ownership
AI3.1	Technology Infrastructure Acquisition Plan	BAI03.04	Procure Solution Components
AI3.2	Infrastructure Resource Protection & Availability	BAI03.03	Develop Solution Components
		DSS02.03	Verify, Approve, & Fulfill Service Requests
AI3.3	Infrastructure Maintenance	BAI03.10	Maintain Solutions
AI3.4	Feasibility Test Environment	BAI03.07	Prepare for Solution Testing
		BAI03.08	Execute Solution Testing
DS12.1	Site Selection & Layout	DSS01.04	Manage the Environment
		DSS01.05	Manage Facilities
		DSS05.05	Manage Physical Access to IT Assets
DS12.2	Physical Security Measures	DSS05.05	Manage Physical Access to IT Assets
DS12.3	Physical Access	DSS05.05	Manage Physical Access to IT Assets
DS12.4	Protection Against Environmental Factors	DSS01.04	Manage the Environment
DS12.5	Physical Facilities Management	DSS01.05	Manage Facilities

Table 3. Inputs & outputs to COBIT 4.1 process PO2, *Define the Information Architecture*

From	Inputs
PO1	Strategic & tactical IT plans
AI1	Business requirements feasibility study
AI7	Post-implementation review
DS3	Performance & capacity information
ME1	Performance input to IT planning

Outputs	To				
Data classification scheme	AI2				
Optimized business systems plan	PO3	AI2			
Data dictionary	AI2	DS11			
Information architecture	PO3	DS5			
Assigned data classifications	DS1	DS4	DS5	DS11	DS12
Classification procedures & tools	*				

* Outputs to outside COBIT

Detailed response

COBIT 4.1 Process PO2: Define the information architecture

COBIT 5 Management Practice: APO03.02, Define reference architecture
COBIT 5 Management Practice: APO01.06, Define Information (data) & System Ownership

All 4 control objectives of *PO2, Define the information architecture*, are incorporated into these 2 management practices of COBIT 5. Sunera observed several deficiencies in ITD's services in this area, including:

- The application architecture has not been used in the IT planning process
- The City does not have an enterprise data dictionary
- Data is not classified at the City
- The City lacks critical policies relevant to this control objective.

Their recommendations include:

- Continue planning to convert the application architecture to database format
- Utilize the current state application architecture to support future analysis and decisions to optimize the creation, use and sharing of information by the business
- Compile existing data dictionaries from application design documentation and system interface documentation to form the initial enterprise data dictionary
- Develop a data classification scheme
- Develop policies for:

- System access provisioning and monitoring
- Information security
- Restricting developer access to production systems
- Governance of system and database administration.

ITD response

Since the audit ITD has made extensive progress in this area.

- We have converted the application architecture to database format
- We are using the application architecture in tactical planning, and are now planning to integrate the architecture into the change management process
- We have incorporated information and system ownership into the application architecture
- We have developed policies for information security and governance of system and database administration
- The enterprise data dictionary remains a future target; as ITD replaces legacy applications the new applications will integrate with the data warehouse and business intelligence tools. ITD limits the projected scope of the enterprise data dictionary to those applications using the data warehouse
- As part of the PCI compliance effort, ITD has begun to identify sensitive data and restrict access to it, and has developed policies to enforce those restrictions; a formal data classification scheme remains a future target
- Policy development for system access provisioning requires collaboration with Human Resources and Security Departments; that remains a future target
- Restricting developer access to production systems and developing the enforcing policies efforts are limited by staffing; increased logging of access and greater oversight by change management is ITD's workaround for this deficiency.

COBIT 4.1 Process AI3: Acquire & maintain technology infrastructure

COBIT 5 Management Practice: BAI03.03, Develop Solution Components
COBIT 5 Management Practice: BAI03.04, Procure Solution Components
COBIT 5 Management Practice: BAI03.07, Prepare for Solution Testing
COBIT 5 Management Practice: BAI03.08, Execute Solution Testing
COBIT 5 Management Practice: BAI03.10, Maintain Solutions
COBIT 5 Management Practice: DSS02.03, Verify, Approve, & Fulfill Service Requests

The 4 control objectives of process AI3 are reorganized across 6 management practices in COBIT 5. Sunera observed deficiencies in this area of control.

- The City does not have a formal set of information technology standards
- The City's control environment lacks critical policy, procedure, and guideline documentation
- The City does not have development and test environments to support effective and efficient feasibility and integration testing of infrastructure components

Sunera's recommendations were:

- Update the City’s information technology standards to include technology infrastructure
- Develop and implement a procedure to monitor capacity and utilization of key network and system resources
- Establish technology infrastructure development and test environments.

ITD response

- The technology infrastructure is in transformational change: the introduction of Voice-over-IP (VoIP), the 800 MHz radio system rebanding, replacement of the entire network infrastructure, and the introduction of virtual switches into our VMWare ESX environment, cause ITD to wait until these projects are complete, when we shall document fully the new technologies and publish them as a complete set of City standards.
- ITD is researching for a unified system to monitor capacity, utilization, other operational parameters, and seeking sufficient funding to acquire it. We can and do monitor parameters for many systems, but with an almost equal number of tools, requiring considerable, and expensive, human oversight. An intelligent, automated system integrating information from many systems would free staff to perform higher-value tasks, and provide better event correlation and response.
- Development and test environments exist or we can create them for applications in our virtual platform. Many of our legacy systems reside on older, very expensive, equipment, the cost of which precludes duplication for any purpose. ITD is replacing these applications with new, virtualized ones; development and test environments are the standard approach for all future systems.

Appendix A – COBIT 4.1 and 5 maturity levels

COBIT 4.1 Maturity Model Level	Process Capability (COBIT 5)
5 Optimized – Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.	**Level 5: Optimizing process –** The level 4 predictable process is continuously improved to meet relevant current and projected goals.
4 Managed and measurable – Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice Automation and tools are used in a limited or fragmented way.	**Level 4: Predictable process –** The level 3 established process now operates within defined limits to achieve its process outcomes.
3 Defined process – Procedures have been standardized and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalization of existing practices.	**Level 3: Established process –** The level 2 managed process is now implemented using a defined process that is capable of achieving its process outcomes.
	Level 2: Managed process – The level 1 performed process is now implemented in a managed fashion (planned, monitored, and adjusted) and its work products are appropriately established, controlled, and maintained
2 Repeatable but intuitive – Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.	**Level 1: Performed process –** The implemented process achieves its process purpose.
1 Initial/*Ad hoc* – There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There, however, no standardized processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.	
0 Non-existent – Complete lack of any recognizable processes. The enterprise has not even recognized that there is an issue to be addressed.	**Level 0: Incomplete process –** The process is not implemented or fails to achieve its purpose.

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