Information Technology Risk Assessment

City of Tulsa Internal Auditing

June 2011

Information Technology Risk Assessment

City of Tulsa Internal Auditing

Ron Maxwell, CIA, CFE
Chief Internal Auditor

Clift Richards, CPA
City Auditor

AUDIT TEAM:
Cecilia Ackley, CPA, Internal Audit Manager
Nathan Pickard, CIA, CISA, IT Auditor

Information Technology Risk Assessment
June 2011

Audit Purpose

The purpose of this project was to identify high-risk information technology (IT) areas and develop an IT audit plan to address those areas.

Summary

The City has come to rely extensively on technology in almost every service it provides. Information technology has become the single highest risk area in many large organizations. The City of Tulsa has over 120 IT employees and supports more than 125 different applications used by City employees. These applications require support of a diverse technology infrastructure. Assessing risks within the IT department has never been more important.

Internal Auditing used Control Objectives for Information and Related Technology (COBIT) and other tools to develop a repeatable risk assessment process. Internal Auditing developed an online survey to assess the IT risks faced by the City. This year the survey focused on IT processes and projects. Future assessments will include IT applications and infrastructure.

For IT Processes, we ranked the risks according to reliability and efficiency, consistency, technology leverage, results management, human capital, complexity, strategic impact, operational impact, legal/regulatory compliance, and financial reporting.

For IT projects, we ranked the risks according to criticality, experience, executive ownership, process re-engineering, development platform, custom programming, project budget, strategic impact, operational impact, legal/regulatory compliance, and financial reporting.

Audit Plan

Based on the risk assessment, Internal Auditing has identified seven potential audit options listed below:

- Project Management Office – IT engagement process
- Human Resources Information Systems – time & attendance project
- Assess and manage IT risks
- Manage third-party services process
- Monitor and evaluate internal control process
- Automated solutions process
- Define the information architecture process

Ranking Results

Appendix A includes the detailed results of our risk assessment on IT processes. Appendix B includes the results of our risk assessment on IT projects.

Appendix A - IT Processes Risk Ranking

	Process Information		Final Risk Ranking	
Count	Process Name	Process Description	Overall Risk Score	Risk Ranking Overall
1	**PO9 Assess and manage IT risks.**	A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organization caused by an unplanned event is identified, analyzed and assessed.	2.83	High
2	**DS2 Manage third-party services**	The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance.	2.83	High
3	**AI4 Enable operation and use**	Knowledge about new systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.	2.58	High
4	**DS7 Educate and train users**	Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results.	2.58	High
5	**ME2 Monitor and evaluate internal control.**	Establishing an effective internal control program for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews.	2.58	High
6	**AI2 Acquire and maintain application software**	Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards.	2.46	High
7	**AI1 Identify automated solutions**	The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach. This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to 'make' or 'buy'.	2.42	High
8	**PO7 Manage IT human resources**	A competent workforce is acquired and maintained for the creation and delivery of IT services to the business. This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating.	2.42	High
9	**AI3 Acquire and maintain technology infrastructure**	Organizations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments.	2.33	High
10	**DS3 Manage performance and capacity**	The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements.	2.29	Medium

Appendix A - IT Processes Risk Ranking

	Process Information		Final Risk Ranking	
Count	Process Name	Process Description	Overall Risk Score	Risk Ranking Overall
11	**PO2 Define the information architecture**	The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimize the use of this information. This encompasses the development of a corporate data dictionary with the organization's data syntax rules, data classification scheme and security levels.	2.25	**Medium**
12	**DS1 Define and manage service levels**	Effective communication between IT management and business customers regarding services required is enabled by a documented definition of and agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels.	2.25	**Medium**
13	**DS9 Manage the configuration**	Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed.	2.25	**Medium**
14	**DS10 Manage problems**	Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions.	2.21	**Medium**
15	**PO1 Define a strategic IT plan**	IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities.	2.21	**Medium**
16	**PO10 Manage projects**	A program and project management framework for the management of all IT projects is established. The framework ensures the correct prioritization and co-ordination of all projects. The framework includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and post-implementation review after installation to ensure project risk management and value delivery to the business.	2.17	**Medium**
17	**DS6 Identify and allocate costs**	The need for a fair and equitable system of allocating IT costs to the business requires accurate measurement of IT costs and agreement with business users on fair allocation. This process includes building and operating a system to capture, allocate and report IT costs to the users of services.	2.17	**Medium**
18	**PO3 Determine technological direction**	The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms.	2.13	**Medium**
19	**AI5 Procure IT resources**	IT resources, including people, hardware, software and services, need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements, and the acquisition itself.	2.13	**Medium**
20	**DS8 Manage service desk and incidents**	Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution.	2.13	**Medium**

Appendix A - IT Processes Risk Ranking

	Process Information		Final Risk Ranking	
Count	**Process Name**	**Process Description**	**Overall Risk Score**	**Risk Ranking Overall**
21	**DS5 Ensure systems security**	The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents.	2.08	**Medium**
22	**ME1 Monitor and evaluate IT performance.**	Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, reporting performance in a timely and systematic manner, and acting promptly upon deviations.	2.08	**Medium**
23	**PO5 Manage the IT investment**	A framework is established and maintained to manage IT-enabled investment programs and that encompasses cost, benefits, prioritization within budget, a formal budgeting process and management against the budget.	2.04	**Medium**
24	**PO8 Manage quality**	A quality management system (QMS) is developed and maintained that includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the QMS by providing clear quality requirements, procedures and policies.	2.04	**Medium**
25	**AI7 Install and accredit solutions and changes**	New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review.	2.04	**Medium**
26	**PO4 Define the IT processes, organization and relationships**	An IT organization is defined by considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organization is embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management.	2.00	**Medium**
27	**ME4 Provide IT governance.**	Establishing an effective governance framework includes defining organizational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.	1.92	**Medium**
28	**DS12 Manage the physical environment**	Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access.	1.83	**Medium**
29	**PO6 Communicate management aims and direction**	Management develops an enterprise IT control framework and defines and communicates policies. An ongoing communication program is implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management.	1.79	**Medium**
30	**DS11 Manage data**	Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of media.	1.79	**Medium**

Appendix A - IT Processes Risk Ranking

	Process Information		Final Risk Ranking	
Count	**Process Name**	**Process Description**	**Overall Risk Score**	**Risk Ranking Overall**
31	**DS4 Ensure continuous service**	The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilizing offsite backup storage and providing periodic continuity plan training.	1.75	**Medium**
32	**DS13 Manage operations**	Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware.	1.67	**Low**
33	**ME3 Ensure compliance with external requirements.**	Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimizing and evaluating the response, obtaining assurance that the requirements have been complied with and, finally, integrating IT's compliance reporting with the rest of the business.	1.67	**Low**
34	**AI6 Manage changes**	All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following implementation.	1.58	**Low**

Appendix B - IT Projects Risk Ranking

	Project Information		Final Risk Ranking *	
Count	**Project Name**	**Project Description**	**Overall Risk Score**	**Risk Ranking: Overall**
1	Public Safety Server, Architecture, and Oracle Migration Project	Replace the Public Safety IBM Servers; Upgrade Oracle database, middleware, and development tools to Release 11g.	2.59	**High**
2	PMO - IT Engagement Process	Develop an engagement process to request projects and resources from the Information Technology Department.	2.50	**High**
3	Sales Tax Rebate	Online processing of Sales tax rebate to comply with Ordinance 21913.	2.46	**High**
4	MFBE & BRIDGE Data Tracking	Track MFBE and BRIDGE utilization from multiple data sources.	2.43	**High**
5	ECM - Permits	Evaluate, purchase, and implement software solution for document management, business process automation, and workflow management in Development Services.	2.39	**High**
6	Voice over Internet Protocol (VoIP)	Migrate the City of Tulsa's telephone system to voice over internet protocol, saving the City thousands of dollars annually in telephone expenses.	2.38	**High**
7	E-Citations - Phase I	Implement a technology solution enabling Tulsa Police Department officers to issue electronic citations.	2.34	**High**
8	Affinity System Hardware and Software Updates	Replace Hewlett Packard Alpha servers and update utility billing software.	2.32	**Medium**
9	TPD - Laptops for police cars	Replacing laptops in Police cars with U1 devices to utilize the cellular network infrastructure.	2.32	**Medium**
10	UCS & Enterprise Work Force and Asset Management	New Enterprise work force and asset management application to replace current antiquated systems.	2.30	**Medium**
11	IT - Department Strategic Plan	A comprehensive outlined plan of standards for the IT Department.	2.30	**Medium**
12	Legal Case Management Software	Provide case tracking software for legal cases involving the City of Tulsa.	2.30	**Medium**
13	Laptops for Fire Department Emergency Response Units - Phase I	Proof of concept to provide a limited number of laptops for field use to so that firefighters can access and record data to Firehouse incident and patient care records and obtain CAD data.	2.23	**Medium**
14	IT - Audit Responses/Reports	Information Technology Department responses to the BKD audit and the three City Of Tulsa internal audits.	2.23	**Medium**

Appendix B - IT Projects Risk Ranking

	Project Information		Final Risk Ranking *	
Count	**Project Name**	**Project Description**	**Overall Risk Score**	**Risk Ranking: Overall**
15	HRIS - Employee ID Number	Replaces employee ID's (which are currently employee SSN's) with a new computer generated employee ID. Internal and external dissemination will contain the employee ID only to protect employee identity.	2.20	**Medium**
16	ECM - Contact and Agenda Management for the Office of the City Council	Assess and recommend a contact and agenda management solution for the Office of the City Council.	2.16	**Medium**
17	TriTech VisiCAD	Acquisition and implementation of new Computer Aided Dispatch system for 911.	2.13	**Medium**
18	Sales Tax Collection	Collection of Tulsa Sales Tax.	2.13	**Medium**
19	HRIS - Time & Attendance - Phase I	Implement time and attendance for the 911 Emergency Call Center.	2.13	**Medium**
20	TPD - In-Car Video System	Installation of video cameras in marked Police squad vehicles.	2.13	**Medium**
21	GIS/GPS for Development Services	Display permitted construction projects on a moving map allowing inspectors to do code enforcement as they travel around the city.	2.05	**Medium**
22	800 MHz rebanding - Wave 2	Reprogram all radios for frequency changes.	2.00	**Medium**
23	Police Forensics Laboratory Information System	Purchase and implement a LIMS for the Forensics Lab.	1.98	**Medium**
24	HRIS - Resumix Replacement	Assess replacement of Human Resources' Resumix software.	1.93	**Medium**
25	HRIS - Phase I (eAdvice)	Develop a process for generating electronic pay advices and storing them on a secure server. Access will be controlled by a secure website using individual logins.	1.79	**Medium**
26	Zoo Transition	Transition IT support functions of the Zoo to private management company.	1.79	**Medium**
27	City Medical System Replacement	Medical office software upgrade to comply with HIPPA regulations.	1.73	**Medium**
28	Mass Notification System	A hosted solution for emergency messaging to households and businesses in the Tulsa city limits via phone, cell, email.	1.71	**Medium**
29	SharePoint 2010	Implement SharePoint 2010.	1.68	**Medium**

Appendix B - IT Projects Risk Ranking

	Project Information		Final Risk Ranking *	
Count	Project Name	Project Description	Overall Risk Score	Risk Ranking: Overall
30	IT - Security	A comprehensive outlined plan of security standards for the IT Department.	1.66	Low
31	CS - Salary Projection	Salary projection for budget planning.	1.63	Low
32	TPD - VisionTEK Frontline Upgrade	Upgrade Police laptops with latest Frontline software, which requires a hardware upgrade of existing laptops to U1 devices.	1.63	Low
33	Fire Hydrant Inspections	Implement automated workflow for management and tracking annual Fire Hydrant Inspections.	1.61	Low
34	PW Automated Dispatching and Scheduling	Provide an automated solution for establishing scheduled meter reading routes and dispatching water meter readers for Public Works Field Customer Service.	1.61	Low
35	PMO - Methodology & Templates	Establish the IT Project Management Office (PMO).	1.55	Low
36	ECM - SDVM	Provide content management application for scanned work orders. (SD#51808)	1.52	Low
37	Bring IT Home Tulsa	Bridge the technology gap by providing computers and internet connectivity to mid and low income families and communities.	1.48	Low
38	IT - Disaster Recovery / Business Continuity Planning	Create a comprehensive disaster recovery plan for Information Technology systems and applications. The plan will document how the Disaster Recovery process will be accomplished when funding is available.	1.46	Low
39	CAD 911 Reports	Redevelop Computer Aided Dispatch 911 report used by Tulsa Fire Department for response time analysis.	1.36	Low
40	IT - Business Continuity for Utility Billing	Provide assistance to Utility Billing in defining a business continuity plan in the event that the Utility Billing system is compromised.	1.34	Low
41	IT - 911 Business Continuity	Obtain a backup center for 911 operations.	1.20	Low

* Project list as of 2/17/2011

Distribution List:

Mayor Dewey Bartlett
Councilor Jack Henderson
Councilor Rick Westcott
Councilor Roscoe Turner
Councilor Maria Barnes
Councilor Chris Trail
Councilor Jim Mautino
Councilor John Eagleton
Councilor Bill Christiansen
Councilor G. T. Bynum
City Auditor Clift Richards
Chief of Staff Terry Simonson
City Manager Jim Twombly
Council Administrator Don Cannon
Council Secretary Dana Burks
Chief Information Officer Ben Stout
Director, IT Information Services Tom Golliver
Director, IT Operations and Support Blaine Young
Manager, IT Administration and Planning Rick Lisenbee
Director of Finance Mike Kier
Senior Administrative Services Officer Wendy Martin
External Auditor
Mayor’s Advisory Audit Committee