CITY OF Tulsa
A New Kind of Energy.

Manage Third Party
Information Technology Services

City of Tulsa Internal Auditing

June 2013

MANAGE THIRD PARTY

INFORMATION TECHNOLOGY SERVICES

City of Tulsa Internal Auditing

Ron Maxwell

Ron Maxwell, CIA, CFE
Chief Internal Auditor

Clift Richards

Clift Richards, CPA
City Auditor

AUDIT TEAM:

Cecilia Ackley, CPA Internal Audit Manager
Mary Ann Vassar, CPA

INTRODUCTION

The City of Tulsa Information Technology Department (ITD) deals with a significant number of third party service providers to perform a wide variety of automated processes used by both internal departments and citizens/taxpayers. Third party service management and monitoring is critical to ensure service, recordkeeping, collection and payment processes operate securely, efficiently and effectively. City ITD management recognizes this area's importance, and recently began efforts to centralize monitoring and maintenance of such vendors in the Administration and Planning function.

SCOPE

The scope of this engagement was to review the process of managing ITD related third-party services.

OBJECTIVES

The objectives of the Manage Third Party Services audit included the following:

- Determine if all ITD third party services are identified
- Review management of ITD supplier relationships
- Determine if ITD supplier risks are being considered
- Review the amount of ITD supplier monitoring being performed

CONCLUSION

The Internal Auditing department conducts audits in conformance with the International Standards for the Professional Practice of Internal Auditing. Those standards require the audit is planned and performed to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on the audit objectives.

Formal third party service management processes are not sufficient to perform audit tests or reach reasonable findings and conclusions. Due to this, we have assessed which process areas need development to achieve COBIT 4.1 (Control Objectives for Information and Related Technologies) objectives. These areas are detailed in the following Observation section of this report. One observation relates to the general framework and process needed, while the second observation focuses on specific risks for cloud-computing based vendor services.

The ITD response to these observations is framed in the context of its larger supply chain management development effort, which includes management of third party services. Internal Auditing plans to track development of these remaining third party service items through our continuous Report on Management Action (ROMA) efforts. ITD's audit response states these processes are planned for substantial completion by the start of fiscal year 2015. A follow up audit of the manage third party services process will be considered at that time.

OBSERVATION

City Information Technology Department (ITD) third party service management processes are under development, but not completed or implemented.

To effectively evaluate the internal controls and processes related to third party service management, Internal Audit selected Control Objectives for Information and Related Technologies (COBIT) 4.1, which describes specific ITD processes and controls to manage third party services. These are:

- Identifying and categorizing supplier services
- Identifying and mitigating supplier risks
- Monitoring and measuring supplier performance

City third party suppliers are substantially identified and partially categorized. Informal third party supplier monitoring is occurring. Automated contract expiration monitoring is in development, and some critical applications are identified and have contingency plans. An Information Technology Security Board (ITSB) including ITD, Security and Purchasing personnel is developing processes, policies, activities, communication plans, roles and responsibilities to address the following items:

- Identification, ranking, and analysis of suppliers, including criticality
- Evaluation, measurement and mitigation of vendor risks
- Quantifying standards/requirements for supplier selection
- Vendor performance measurement - including performance analysis, processes, communication, performance objectives, deliverables, metrics, and deadlines/triggers for critical vendors. A vendor assurance questionnaire has been developed.

Lack of a third party service management process may result in:

- Unknown or undetected supplier communication or testing efforts
- Omitted internal actions and responses, including those needed by non-ITD users
- Undetected or unresolved substandard performance
- Vendor contract lapses, which may result in cost increases
- Unintended or incorrect contract renewal or omitted technical specifications
- Unidentified and/or unmitigated vendor risk, causing critical service interruptions

RECOMMENDATION

We recommend ITD management continue efforts to develop a vendor monitoring and measurement process, and that these efforts receive priority attention. Remaining areas to be addressed include:

- Detailed vendor management monitoring, communication, roles and tasks, including roles for non-ITD users of various applications/systems
- Guidance (policies and procedures) for monitoring methods to be used
- Identification, assessment and documentation of all critical vendors
- Identification and analysis of vendor sustainability and performance risks (for critical vendors at a minimum),
- Evaluation and development of mitigation for likely and/or high impact risks (such as contingency plans, alternate vendors/suppliers, etc.)

- Definition and documentation of vendor deliverables/metrics to measure and monitor vendor performance (for critical vendors at a minimum)
- Documentation and analysis of vendor performance history (for critical vendors at a minimum) to assess long-term vendor effectiveness

We recommend more formalized project management be implemented to ensure vendor management development progress. This will clarify and monitor the project's scope, charter, completion timelines, tasks and resource expectations.

OTHER OBSERVATION:

On Demand/Shared Network Data Vendor Management

An additional area of third party service management relates to vendor-provided 'on demand' shared network ITD resources, also referred to as 'cloud' computing. Electronic pay advice and automated time/attendance service vendors are 'cloud' based vendors. Due to the ITD processes and structure under review at this time by City and ITD management as well as an external consulting team, it is relevant to proactively consider some unique features and management aspects of third party 'cloud' services.

Considerations unique to cloud environments include, (but are not limited to):

- Changed security risk for desktop and mobile devices due to multiple data tenants and locations (including potential foreign country locations and data subcontractors)
- Possible changes to contract scope, service level agreements, roles and accountabilities due to cloud processing and/or infrastructure
- Ultimate data ownership, recovery and transfer in the event of service provider(s) closure, contract termination, or physical disaster
- Controls and safeguards protecting data/transactions - including:
    - SOC (Service Organization Control) reports verifying security, confidentiality, and privacy,
    - protection from subpoenas of other tenants' data, and
    - security and vulnerability testing on the cloud environment
- Limitations or costs for forensic data requests (used for investigations/analysis/audits)
- Potential impact on compliance requirements (dependent on the nature of cloud processed/stored data)
- Vendor requirements for notifying customers when locations or security practices change

The Information Technology Security Board (ITSB) has incorporated aspects of cloud vendor risk evaluation in its draft of a Supplier Assurance Questionnaire. Aspects of monitoring cloud infrastructure and security, including policies, procedures, personnel roles, contract standard terms and possible compliance impacts have not yet been developed. Guidance on the evolving field of cloud security and controls is available from the Cloud Security Alliance, as well as ISACA (Information Systems Audit and Control Association) and the IIA (Institute of Internal Auditors).

RECOMMENDATION

We recommend that IT continue to consider cloud-based data service vendor control and security issues while developing the third party vendor management process.

INFORMATION TEHCNOLOGY DEPARTMENT RESPONSE

INTRODUCTION

Because the City of Tulsa's Information Technology Department (ITD) provides services to all City departments, external entities, and citizens, the reliability and quality of its supply chain is critical to all municipal operations. While ITD has endeavored to manage its complete supply chain, recent challenges have demonstrated the importance of centralized, comprehensive vendor management and assurance processes. ITD is therefore undertaking a new initiative to manage its supply chain through documented standards and frameworks to ensure the availability, reliability, and quality of services provided to the city. The frameworks being incorporated into ITD's new processes are:

COBIT 5
ITIL v3 2011, Supplier management
NIST Interagency Report 7622, Notational Supply Chain Risk Management Practices for Federal Information Systems

These three frameworks encompass the areas of governance, service management, and security for the ITD supply chain.

The Internal Auditing Department (IAD) has performed an audit on third party service management for information systems. Their auditing standard was the DS2 Manage Third-party Services process of COBIT 4.1. ITD has begun to adopt COBIT 5 as a governance and management framework. Therefore, this response to the IAD report uses the corresponding COBIT 5 process, APO10 Manage Suppliers, as its reference.

RESPONSE TO OBSERVATION

While the IAD audit limits its scope to the COBIT process DS2, ITD has taken a broader approach to ensure the success of its vendor management and assurance efforts. ITD is assembling an application portfolio, mapping applications to their supporting infrastructure and the business services which use them. This process, supporting COBIT 5's APO03 Manage Enterprise Architecture, identifies the dependencies between end-to-end service components (applications, servers, network, security, client hardware and software), and through that, identifies and prioritizes supply chain relationships based on their importance to the City's various services.

The first step in managing the supply chain is choosing the right supplier. Many of ITD's projects are software acquisitions. The members of the Project Management Office (PMO) and other ITD staff have received specialized training in gathering business requirements. Studies have documented the cost of poor requirements in both system and supplier performance. ITD will continue to improve its requirements specification process, targeting COBIT 5's BAI02 Manage Requirements Definition process, to avoid issues and improve system and supply chain performance.

The Information Technology Security Board (ITSB) has begun assessing supply chain risk, and is working with Purchasing to collect a Vendor Assurance Questionnaire from all prospective ITD vendors. This Questionnaire will be used to assess the information security risk of vendor products and services. Critical suppliers will receive additional scrutiny, including examination of SSAE16 or equivalent documentation. Operational aspects of information security and supply chain risk will use NIST IR 7622 as guidance. ITD will recommend to the ITSB and subsequently, to Purchasing, that the Questionnaire be required in all appropriate procurements, including those made by non-ITD users.

Additionally, ITD has centrally assigned contract management responsibilities, and is presently developing a formal supply chain management program in cooperation with Purchasing. This ITIL- and COBIT-compliant program will establish Key Performance Indicators (KPIs) and evaluation procedures to correct and improve supplier performance throughout the term of the respective contract.

RESPONSE TO OTHER OBSERVATION

ITD has begun exploring application hosting models other than "on premise" (including vendor-hosted and Software-as-a-Service). The use of these models is still evolving and ITD will remain conscientious of information security, performance, and reliability. The department is using guidance provided through publications by ISACA (IT Control Objectives for Cloud Computing, 2011), the National Institute of Standards and Technology (NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, 2011), and the Cloud Security Alliance (Security Guidance for Critical Areas of Focus in Cloud Computing, v3.0, 2011).

CONCLUSION

The importance of ITD supply chain management continues to grow. Software acquisition outpaces internal programming and development. The City's business units' dependence on information technology increases as their services evolve, becoming more sophisticated and complex. In this environment, ITD's responsibility to the City includes vigilant management of its supply chain to meet the needs of the City and protect its information technology resources. The Department's initiatives for controlling and managing its supply chain will provide increased reliability and security of these assets, and will enable all departments to meet the changing needs of the citizens of Tulsa. ITD will have all parts of its supply chain management program in place by the start of fiscal year 2015.

ITD appreciates the IAD's report on managing third party information services and considers IAD's recommendations closely aligned with its own vision for the new vendor management and assurance processes. The Department recommends this critical topic be a prominent feature in future ITD audit plans.

DISTRIBUTION LIST

Mayor
Councilor, District 1
Councilor, District 2
Councilor, District 3
Councilor, District 4
Councilor, District 5
Councilor, District 6
Councilor, District 7
City Auditor
Chief of Staff
City Manager
Council Administrator
Council Secretary
Finance Director
Sr. Admin. Services Officer
Chief Technology Officer
Director of Operations & Support — IT
Director of Applications — IT
External Auditor
Mayor’s Audit Committee
Internal Audit Staff