CITY OF Tulsa
A New Kind of *Energy*™

Electronic Pay Advice (Continuous Monitoring Payroll Audit)

City of Tulsa Internal Auditing

January 2013

Electronic Pay Advice (Continuous Monitoring Payroll Audit)

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, Senior Auditor
Lela Walden, CPA, Staff Auditor

INTRODUCTION

The City of Tulsa began providing electronic pay advice information to employees and retirees in January 2012 through National Payment, a data service vendor selected through the Purchasing request for proposal process. Detailed pay information is now provided to City employees through a National Payment website. At calendar year end 2012, employees' annual W-2 wage and earnings statement information will be made available using this same vendor and online service.

Employee payroll information is transmitted electronically to the vendor by the Central Payroll department each pay period. Central Payroll is part of the Finance Department and is responsible for providing timely and accurate pay information to employees.

SCOPE

The scope of this engagement was limited to electronic pay advice processing, pay data transmittal and pay information availability. Pay information access controls were tested, and data maintenance security assurance was also reviewed. Internal Auditing used data analytic tools to examine Payroll department transmittal and vendor receipt for 100% of over 22,000 pay advice records in five pay periods. Consistency of the review performed by Payroll management to ensure error correction and timely, consistent availability of pay data was also tested. In addition, controls to monitor and ensure the security of sensitive employee identification information were also assessed.

OBJECTIVES

The objectives of the Electronic Paystub Advice Payroll Audit included the following:

- Determine payroll information is accurately and completely transmitted to the pay advice vendor.
- Ensure payroll information is provided consistently and timely to the pay advice vendor and employees.
- Ensure sensitive employee identification information is securely transmitted, stored and accessible only to authorized employees and intended Payroll management.

AUDIT METHODOLOGY AND PROCEDURES

Internal Auditing used standard audit methodology including interviews, observations, and substantive testing in the performance of this audit.

Data analytic tools were used to test the transmission of 100% of over 22,000 employee pay advices for the five pay periods in the first and second quarter of calendar year 2012. These tests confirmed employee and retiree pay information had been consistently and timely transmitted to and received by the vendor from January 2012 through June 2012.

Review of vendor records and online pay advice history determined that electronic pay advices had been published online consistently and timely. Timely, consistent vendor website publication of employee and retiree pay records was confirmed for all periods from implementation in January 2012 through June 2012.

Website controls protecting access to employee pay information were tested. Controls established in the eAdvice web delivery system which:

- require employees to log in to pay advice accounts by establishing unique passwords,
- prevent account access after three unsuccessful log in attempts,
- require accounts to be unlocked by City Service Desk personnel, and
- require unique personal information to reset passwords

were tested and determined to be functioning effectively.

In order to obtain assurance on needed data vendor and City security over sensitive employee identification data, Finance obtained a Statement of Control (SOC) report at Internal Auditing's request. Verification and review of this SOC report was not a part of the vendor evaluation process prior to executing the electronic pay advice services agreement. Further, vendor and City electronic pay stub data security had not been reviewed or assessed prior to our audit. No City procedure to request or periodically update such control reports is currently established. **For further detail, please refer to the Observation Section of this report.**

CONCLUSION

We conducted this audit in conformance with the International Standards for the Professional Practice of Internal Auditing. Those standards require that the audit is planned and performed to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Internal controls over the electronic pay advice process are adequate to ensure pay advice information is accurately, timely and completely transmitted to the pay advice vendor on a consistent basis. Website controls are sufficient to restrict unauthorized access to employee pay and identity information. Initial evaluation and ongoing monitoring of pay advice vendor data security control reports needs improvement.

OBSERVATION

Data Service Vendor Statement of Control Reports

Control Objectives for Information and related Technology (COBIT) specify a needed element of controls over third party service management is identifying and mitigating supplier risk, including conformance with security requirements. Vendor-provided electronic pay stub and W-2 services place security-sensitive employee pay data and Social Security numbers in the custody of third parties.

Effective 6/15/11, Statement on Standards for Attestation Engagements (SSAE) 16 required data service vendors to obtain Service Organization Control (SOC) reports. SOC reports are the only method of independently verifying third party vendor controls over security, confidentiality and privacy of sensitive data. SOC reports also specify user controls needed for the City to maintain adequate security. An SOC report was not obtained from National Payment to assess supplier and City security requirements during the vendor evaluation and proposal process. An SOC report also had not been obtained prior to our audit.

Without the SOC report, the condition and level of vendor pay and W-2 data security had not been assessed at the commencement of our audit. At Internal Auditing's request, Finance obtained an SOC report copy. Based on this report, vendor data security controls were verified and adequate, and specified City user controls are established.

Discussion with Purchasing management determined that omission of SOC report evaluation occurred because requested proposal specifications did not contain this requirement. Additional discussion with the Purchasing Department determined no City-wide requirements exist to establish initial evaluation or ongoing monitoring of SOC reports for City data service vendors.

City Purchasing personnel have indicated that National Payment is not the only vendor with access to City data. Based on vendor information obtained from Purchasing management, all vendors with access to City data have not been formally identified.

Failure to:

1) identify all vendors with City security-sensitive data, and
2) initially obtain SOC reports to evaluate data controls as part of the bidding/quote process, and
3) subsequently monitor vendor data security controls through updated SOC reports

can lead to security exposure of sensitive data. In addition, vendor-specified City internal controls needed to safeguard data may not be identified or established.

RECOMMENDATION

We recommend that vendors with access to City security-sensitive data be identified. In addition, Statement of Control report policies, proposal guidelines, review and monitoring requirements, roles and responsibilities should be developed to assess and monitor data vendor security risk. These requirements need collaboration from both Purchasing and Information Technology departments. Additionally, key City data service user departments should be consulted and involved in developing these requirements and policies.

MANAGEMENT RESPONSES

Mike Kier, Director of Finance
We agree with the recommendation. We have formed an ad hoc committee to implement the recommendations of this report and anticipate completion of the development and implementation of policy and procedures to occur before September 30, 2013.

Major Jonathan Brooks, Information Technology Interim Director
Information Technology agrees with the planned ad hoc committee and related development of policy and procedures.

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
City Manager
Mayor’s Chief of Staff
City Attorney
MRO Director
Council Administrator
Council Secretary
Finance Director
Sr. Admin. Services Officer
Chief Technology Officer
Press Secretary
Controller, Accounting Division
Purchasing Division
Assistant Controller
Payroll Manager
External Auditor
Mayor's Audit Committee
Internal Auditing Staff