Council Auditor's Office

Interim Audit Report on City Payroll Disaster Recovery Procedures

June 11, 2013

Report #735

Released on : July 17, 2013

117 West Duval Street | Jacksonville, Florida 32202-3701 |Telephone (904) 630-1625 | Fax (904) 630-2908
www.coj.net

AUDIT REPORT #735

OFFICE OF THE COUNCIL AUDITOR
Suite 200, St. James Building

June 11, 2013 Report #735

Honorable Members of the City Council
City of Jacksonville

INTRODUCTION

Pursuant to Section 5.10 of the Charter of the City of Jacksonville and Chapter 102 of the Municipal Code, we commenced an audit of the City's payroll office within the Accounting Division of the Finance Department in May 2013. In the early stage of our audit, we identified numerous issues related to the payroll-related disaster recovery procedures. Section A7.02 of the Government Auditing Standards emphasizes the timely issuance of the report as an important reporting goal for auditors and permits providing interim reports of significant matters to appropriate entity officials. Such communication alerts officials to matters needing immediate attention and allows them to take corrective action before the final report is completed. The issues we discovered during the preliminary stage of our audit appeared to be significant. Moreover, communicating findings on disaster recovery procedures in a timely manner to the management appeared to be necessary given that our work coincided with the official start of hurricane season (June 1). Therefore, we chose to issue an interim report on the payroll-related disaster recovery procedures. We will continue our audit of the City's payroll office and issue a final report once the remainder of our audit work is completed.

STATEMENT OF OBJECTIVE

To determine if internal controls related to the disaster recovery procedures for the City's payroll are in place.

STATEMENT OF SCOPE AND METHODOLOGY

The scope of our audit for the objective related to the disaster recovery procedures was the present period when our initial review of the payroll procedures was conducted (May-June 2013). We interviewed applicable personnel and reviewed supporting documentation provided by various parties. Once we identified a few issues with the disaster recovery procedures, we focused on conducting additional interviews and reviewing disaster recovery procedures in detail since it is a significant issue requiring the immediate attention of management. We acknowledge that more issues related to the disaster recovery procedures could be discovered after this interim report is issued; if discovered, we will include those findings in the final report.

Our report is structured to identify Internal Control Weaknesses, Audit Findings, and Opportunities for Improvement as they relate to our audit objectives. Internal control is a process implemented by management to provide reasonable assurance that they achieve their objectives in relation to the effectiveness and efficiency of operations and compliance with applicable laws and regulations. An Internal Control Weakness is therefore defined as either a defect in the design or operation of the internal controls or is an area in which there are currently no internal controls in place to ensure that objectives are met. An Audit Finding is an instance where management has established internal controls and procedures, but responsible parties are not operating in compliance with the established controls and procedures. An Opportunity for Improvement is a suggestion that we believe could enhance operations.

STATEMENT OF AUDITING STANDARDS

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

AUDITEE RESPONSES

Responses from the auditee have been inserted after the respective finding and recommendation. We received these responses from the Finance Department, via C. Ronald Belton, Assistant to the Mayor, Chief Financial Officer, and the Information Technology Division, via Usha Mohan, Division Chief ITD, Chief Information Officer, in a memorandum dated July 17, 2013.

AUDIT CONCLUSION

Internal controls related to the disaster recovery procedures for the payroll-related activities are not adequate and need to be immediately reviewed and modified by management to ensure that sensitive payroll data is protected and that payroll is run in a timely and accurate manner in the event of an emergency. In our opinion, a contributing factor to these problems is that the Comptroller and Payroll Manager positions remain vacant; therefore, direct oversight of these areas is lacking.

AUDIT OBJECTIVE

To determine if internal controls related to the disaster recovery procedures for the City's payroll-related activities are in place.

Finding 1 *Failure to Adequately Safeguard Sensitive Payroll Data*

While reviewing the disaster recovery procedures for payroll, we found that the sensitive payroll data of City's employees was not adequately safeguarded. The City's payroll office currently keeps three disaster recovery backup flash drives containing sensitive payroll data of all City employees. Each flash drive should contain three files: direct deposit file, check file, and child support file. The direct deposit file includes the following data on all employees who receive direct deposit: names, employee identification numbers, bank account numbers, and amounts to be paid. The check file includes the following data on all employees who are not enrolled in direct deposit: names, addresses, salaries and wages, and deductions withheld. Finally, the child support file includes the following data on all employees who pay child support: names, social security numbers, and amounts to be paid.

We found various issues related to the safeguarding of sensitive payroll data in the disaster recovery procedures listed below:

1. Flash drives were not password protected.
2. Data on the flash drives was not encrypted.
3. The safe at the City's payroll office where one of the flash drives is kept was not locked on two separate occasions.
4. One of the flash drives was held at the Central Payroll Technician Senior's home, although the employee was not capable of transmitting the direct deposit file to the bank from home since she was not provided with a City laptop with necessary encryption software installed on it. Finally, the Information Technology Division was not aware of the fact that there was a third flash drive that was kept at the Central Payroll Technician Senior's home.
5. One of the flash drives was physically walked from City Hall to the City's Emergency Operations Center and back every other month.

It should be noted that all three flash drives were confiscated and purged by the City's Security Officer in the Information Technology Division after issues listed above were brought to his attention which confirm the legitimacy of our concerns about the safety of this sensitive payroll data.

Recommendation to Finding 1

We recommend the City's payroll office and the Information Technology Division work together to determine how to adequately safeguard the sensitive information of the City's employees while remaining prepared to process payments of salaries and wages in the event of an emergency in a timely and accurate manner. In particular, we recommend abandoning usage of flash drives and instead relying on the Oracle system used by the City's payroll office to provide payroll files on demand in case of emergency. Finally, to plan for a situation when Oracle is not available, management should consider arranging an agreement with the bank and other involved third parties in which the latest payroll file submitted by the City is used to process payroll payments in case of emergency.

Auditee Response to Finding 1

Agree ☒ Disagree ☐ Partially Agree ☐

The City's Payroll, Information Technology and Treasury Divisions are working together toward developing a new process of maintaining pay transmittal data and encryption keys directly on the Oracle servers in the data center for normal and emergency operations which will maintain pay data in a secure location. We will keep the Council Auditor's Office updated as progress is made. The City's banking services provider is able to reuse a historical payroll ACH file from 1-90 days old. They have also offered the additional functionality of receiving an ACH file for transmission up to 45 days in advance of the effective pay date.

Finding 2 *Issues with City's Ability to Transmit Direct Deposit File to the Bank*

Currently, in the event of an emergency, the City would encounter various difficulties with submitting a direct deposit payroll file to the bank for salaries and wages to be sent to employees' accounts. The direct deposit payroll file could be downloaded from Oracle at any time. The City also keeps copies of this file on three flash drives in case Oracle is not available. Three flash drives are kept at three different locations: Emergency Operating Center (EOC), City's payroll office at City Hall, and Central Payroll Technician Senior's home. To send a file to the bank, one has to encrypt it. Special software has to be installed on a computer to complete encryption. Finally, one would also need to have access to the bank's website to transmit the file.

We found various issues with the current disaster recovery procedures on submitting direct deposit file to the bank via flash drive method:

1. Sending the direct deposit file from the EOC has not been possible since March 6, 2013. The EOC computer utilized to process the direct deposit file in the event of an emergency has been replaced. The software necessary for payment processing has not been installed on the new computer at the EOC, and there is also an issue with the IP (Internet Protocol) address that has not been addressed.
2. Sending the direct deposit file from the Central Payroll Technician Senior's home is not possible since she does not have a City's laptop with the encryption software installed on it.
3. At City Hall, three employees currently have encryption software installed on their computers. However, one of three employees' computers on which encryption software was installed at some point could no longer be used to submit the file to the bank. The last time this employee successfully submitted the file was in early 2012. Due to a reduction in personnel, this employee has recently tried to submit the file to the bank, but discovered that there was an issue with the encryption software.
4. Of the two remaining employees at City Hall who have access to the bank's website and have properly functioning encryption software installed on their computers, one has never submitted the file to the bank in the past as she is not a payroll employee.

Recommendation to Finding 2

We recommend the City's payroll office and the Information Technology Division immediately address this issue and work together to ensure that submission of the direct deposit file to the bank in case of emergency could be completed at any time by more than one person from more than one location.

Auditee Response to Finding 2

Agree ☒ Disagree ☐ Partially Agree ☐

The Payroll, Treasury and Information Technology Divisions have been working to update the new computers in the EOC center with the bank encryption keys and required programs to enable remote processing and transmittal of the payroll Direct Deposit File to the bank. We will test the current EOC procedures to ensure smooth operations in the event of an emergency. The City's banking services provider is able to reuse a historical payroll ACH file from 1-90 days old. They have also offered the additional functionality of receiving an ACH file for transmission up to 45 days in advance of the effective pay date. Upon availability of encryption capabilities on the Oracle server, new procedures and processes will be updated and implemented.

Finding 3 *Inconsistencies Between Current Practices and Standard Operating Procedures*

Current practices regarding the processing of salaries and wages in the event of an emergency do not reflect the written standard operating procedures (SOPs).

1. Disaster recovery backup files are prepared every two months while SOPs state the files should be prepared each month. No log is kept documenting when back up files on each of three flash drives are updated.
2. SOPs state one backup flash drive is to be kept in the safe at the City's payroll office in City Hall and another in the safe at the Emergency Operating Center. However, there was a third flash drive that was kept at the Central Payroll Technician Senior's home.
3. SOPs state the City's payroll office can submit the direct deposit file to the City's bank from any computer. In fact, only computers with the appropriate software installed by the Information Technology Division can submit the direct deposit file to the bank.

Recommendation to Finding 3

We recommend the City's payroll office and the Information Technology Division review the current standard operating procedures in place to determine if they are adequate, up-to-date and followed by personnel.

Auditee Response to Finding 3

Agree ☒ Disagree ☐ Partially Agree ☐

The most recent Payroll Disaster Recovery procedure was updated as of May 25, 2012 and is under review. The current procedures will be reviewed and tested with payroll personnel to

ensure proper computer access and program functionality to encrypt and transmit payroll data. Upon implementation of encrypted files on the Oracle server, updated policies and procedures will be issued and implemented.

Opportunity for Improvement 1 *Updating Payroll Disaster Recovery Backup Files Biweekly*

The City has the opportunity to update the backup payroll data files more regularly. Currently, the City's payroll office updates the disaster recovery backup file every two months, although standard operating procedures state the update should occur every month. Updating files on a more regular basis would decrease the possibility of occurrences of new hires not being paid and recently terminated employees being paid, and would ensure that recent changes in pay are reflected in pay for current employees in case of emergency.

Recommendation to Opportunity for Improvement 1

We recommend the City's payroll office and the Information Technology Division work together to determine the City's costs and benefits of updating payroll backup files on a biweekly basis.

Auditee Response for Opportunity for Improvement 1

Agree ☒ Disagree ☐ Partially Agree ☐

Finance and ITD have reviewed the process of creating the strip file and have determined that, the cost exposure on a 2 month old file and the resources necessary to create the file was a greater risk and cost than using a more current non-stripped version. Therefore, in the future, the City will rely on our disaster recovery providers to pay individuals in the event of a disaster. This is an improvement to current processes and we thank the Council Auditors for this opportunity to leverage their findings to make these improvements.

We appreciate the assistance and cooperation we received from the Finance Department and the Information Technology Division during the initial phase of our audit.

Respectfully submitted,

Kirk A. Sherman, CPA
Council Auditor

Audit Performed By:

Kim Taylor, CPA
Elena Korsakova, CPA
Aaron Wilkins