# Richmond City Council

*The Voice of the People.* *Richmond, Virginia*

## OFFICE OF THE CITY AUDITOR

REPORT # 2011-13

AUDIT

*Of the*

# Department of Finance
# ICVerify System

June 2011

## OFFICIAL GOVERNMENT REPORT

*Richmond City Council*
**OFFICE OF THE CITY AUDITOR**
900 East Broad Street, 8th Floor
Richmond, Virginia 23219
804.646.5616 (tel); 804 646.2230 (fax)

*Committed to increasing government efficiency, effectiveness, and accountability on behalf of the Citizens of Richmond.*

# TABLE OF CONTENTS

**Executive Summary**…… i

**Comprehensive List of Recommendations**…… ii

**Introduction**…… 1

**Background**…… 1

**Overall Conclusion**…… 2

Richmond City Council
The Voice of the People. Richmond, Virginia
OFFICE OF THE CITY AUDITOR

# Executive Summary

The City Auditor's Office has completed an audit of general controls for the Finance Department's ICVerify System for the 12-month period ended December 31, 2010.

**Conclusion:**

The controls over data encryption and transmission appear to be designed and operating effectively. However, control deficiencies were noted over data backup, user administration and credit card processing.

**Risks**:

If the deficiencies identified are not addressed, they could lead to:

- Inefficiencies in operations that would impact the essential functions such as duplicate data entry and keying errors
- Credit card data being stolen
- Inappropriate access to the system
- Risk of permanently losing the data if the system suffers interruptions

Management attention is required to address the deficiencies.

The City Auditor's Office appreciates the cooperation of the Departments of Finance, Procurement, and Information Technology staff. Written responses are included at the end of the report. Please contact me for questions and comments on this report.

Umesh Dalal, CPA, CIA, CIG
City Auditor

| # | *COMPREHENSIVE LIST OF RECOMMENDATIONS* | *PAGE* |
|---|---|---|
| 1 | Develop an ICVerify backup policy outlining the requirements for the backup of data and programs. The Policy should include backup frequency, offsite storage, and testing of the backup media. | 3 |
| 2 | Perform tape backups as per the established policy. | 3 |
| 3 | Establish and adhere to a formal process outlining the approval requirements for granting, modifying and removing access to the ICVerify system. | 3 |
| 4 | Work with the vendor to have ICVerify as one of the Tyler Cashiering credit card processing applications. | 4 |

# Summarized Report

## *Introduction*

The City Auditor's Office has completed an audit of general controls for the Finance Department's ICVerify System. This audit covers the 12-month period ended December 31, 2010. The audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and Control Objectives for Information and related Technology (COBIT) guidelines. Those standards provide a reasonable basis for the conclusions regarding the internal control structure over the ICVerify System and the recommendations presented.

## *Audit Objectives*

To determine whether adequate IT general controls for access to programs and data, program changes and computer operations have been established by management to:

- Restrict access to properly authorized individuals
- Ensure that the controls over the systems and related manual processes provide reasonable assurance that:
    - The data entered is complete, accurate, and valid;
    - All data is processed completely and accurately;
    - Data is secured and protected; and
    - System output is protected and distributed properly.

## *Background*

ICVerify is a third party software product that can be used to process all major credit cards. The Revenue Administration Division uses Tyler Cashiering and the Legacy Revenue Collection System (RCS) to process payments for:

- Real estate taxes
- DPU receipts
- Parking tickets
- Animal licenses
- Parking district decals
- City-wide pay-ins

The Tyler Cashiering and the Legacy Revenue Collection System applications utilize the ICVerify software to process credit card payment transactions.

ICVerify is a critical system to the Revenue Administration Division since it is used for processing customer credit card information and holds the sensitive data used. During calendar year 2010, the Revenues Administration Division processed 15,246 credit card transactions.

The current version of ICVerify software (4.04) used by the City meets the requirements for the Payment Application Data Security Standards (PA-DSS). The Standards are a set of requirements to help software vendors and others develop secure payment applications.

***Overall Conclusion:***

***Internal Controls need some improvement***

The controls over data encryption and transmission appear to be designed and operating effectively. However, control deficiencies are noted over data backup, user administration and credit card processing. Management attention is required to address the deficiencies.

**Risks**:

If the deficiencies identified are not addressed, they could lead to:

- Inefficiencies in operations that would impact the essential functions such as duplicate data entry and keying errors
- Credit card data being stolen
- Inappropriate access to the system
- Risk of permanently losing the data if the system suffers interruptions

The following table provides a summary of the findings identified during the audit. The findings are classified into three categories (high, medium and low) based on financial and security risk exposure:

| What did the auditors find? | What is the risk? | How to mitigate the risk? |
|---|---|---|
| *Lack of Daily Backups:*<br><br>ICVerify tape backups are performed only on Tuesdays of each week. Also, there is no periodic backup testing to verify the integrity of the backup tapes and the ability to restore data from tapes.<br><br><u>Best Practice</u><br>The Federal Information System Controls Audit Manual (FISCAM) recommends routinely copying data files and software and securely storing these files at a remote location to mitigate service interruptions. | **Risk Level: High**<br><br>Without proper system backup, the Revenue Administration Division runs the risk of permanently losing some of the data if the system suffers interruptions. | 1. Develop an ICVerify backup policy outlining the requirements for the backup of data and programs. The Policy should include backup frequency, offsite storage, and testing of the backup media.<br>2. Perform tape backups as per the established policy. |
| *Lack of new user access and termination procedures:*<br><br>Management has not documented and communicated<br>➢ The process and associated roles and responsibilities for requesting and approving user access to the ICVerify System.<br>➢ The process and associated roles and responsibilities for terminating access to the ICVerify System.<br><br><u>Best Practice</u><br>COBIT states "Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges." | **Risk Level: Low**<br><br>There is a potential for users to have inappropriate access to information, applications, and infrastructure that are not required for their job responsibilities. This could lead to misuse of the system and data. | 3. Establish and adhere to a formal process outlining the approval requirements for granting, modifying and removing access to the ICVerify System. |

| What did the auditors find? | What is the risk? | How to mitigate the risk? |
|---|---|---|
| *ICVerify is not integrated with Tyler Cashiering:*<br><br>ICVerify is not integrated with Tyler Cashiering. Therefore, credit card details have to be entered twice, once in ICVerify to get the authorization and again in Tyler Cashiering to complete the credit card transaction.<br><br><u>Best Practice</u><br>Payment Card Industry (PCI) Data Security Standard (DSS) is a set of comprehensive requirements for enhancing payment account data security. | **Risk Level:**<br>**Medium**<br><br>Keying in the credit card information instead of swiping the card increases the risk of keying errors. Manual entries also provide an opportunity to steal card data at the cash registers.<br><br>Manual entries slow down the credit card payment process. | 4. Work with the vendor to have ICVerify as one of the Tyler Cashiering credit card processing applications. |

*Legend:*

**High Risk** – Represents major deficiency resulting in significant level of risk. Immediate management attention is required.
**Medium Risk** – Represents control weakness resulting in an unacceptable level of risk that if left uncorrected may deteriorate to a high risk condition.
**Low Risk** – Control weakness exists, but the resulting exposure is not significant.

## MANAGEMENT RESPONSE FORM

## DEPARTMENT OF FINANCE

**ICVerify Audit Report** (Appendix A)

| # | RECOMMENDATION | CONCUR Y-N | ACTION STEPS |
|---|---|---|---|
| 1 | ***Develop an ICVerify backup policy outlining the requirements for the backup of data and programs. The Policy should include backup frequency, offsite storage, and testing of the backup media.*** | Y | New backup policies for all City servers managed by DIT will be developed that include the recommended items. |
| | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| | DIT Director | | 1-Oct-11 |
| | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| | | | |
| | | | |
| # | **RECOMMENDATION** | **CONCUR Y-N** | **ACTION STEPS** |
| 2 | ***Perform tape backups as per the established policy.*** | Y | Backups will be performed to tape as per the policy. |
| | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| | Finance Director & DIT Director | | 1-Oct-11 |
| | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| | | | Memorandum sent to DIT Director on June 6, 2011. |
| | | | |
| # | **RECOMMENDATION** | **CONCUR Y-N** | **ACTION STEPS** |
| 3 | ***Establish and adhere to a formal process outlining the approval requirements for granting, modifying and removing access to ICVerify system.*** | Y | The Director of Finance will request that the DIT Director add ICVerify as an application selection within in the System Access Privilege Request (SAPR) process. The DIT Director will implement the request. |
| | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| | Finance Director & DIT Director | | 1-Jan-12 |
| | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| | | | Memorandum sent to DIT Director on June 6, 2011. |
| | | | |
| # | **RECOMMENDATION** | **CONCUR Y-N** | **ACTION STEPS** |
| 4 | ***Work with the vendor to have ICVerify as one of the Tyler Cashiering credit card processing applications.*** | Y | Department of Finance staff will request updated cost estimate for recommended integration. Request will be submitted as part of the FY 2013 budget process. |
| | **TITLE OF RESPONSIBLE PERSON** | | **TARGET DATE** |
| | Finance Director | | 1-Feb-12 |
| | **IF IN PROGRESS, EXPLAIN ANY DELAYS** | | **IF IMPLEMENTED, DETAILS OF IMPLEMENTATION** |
| | | | |