TO: Mayor and Council Members
FROM: Dona J. Newman, City Auditor
DATE: September 28, 2010
SUBJECT: CRW Post-Implementation Review Report by Transcendent Group

The Transcendent Group was contracted to conduct a post-implementation review of the CRW/TRAK-iT system. Their report is attached along with Management’s Response, which is included in Appendix I.

We would like to thank the City Manager, Information Technology Systems Director, Assistant City Manager, and DCD staff members for cooperation in the preparation of this report.

If you have any questions or concerns, please contact me at 242-3380.

Attachment

xc: Gary R. King, City Manager
    Carl Schwing, Assistant City Manager
    Dolores Menendez, City Attorney
    Rebecca van Deutekom, City Clerk
    John MacLean, ITS Director
    Wayne Howard, HR Director
    Paul Dickson, DCD Building Official
    Audit Committee
EXECUTIVE SUMMARY

Introduction
Transcendent Group has assisted the City Auditor for the City of Cape Coral ("CCC") in providing information technology audit services by performing a post-implementation review of the City's CRW / TRAK-iT system. The post-implementation review was performed during August 2010.

During the 4th quarter of 2009 Transcendent Group assisted the City in performing an IT risk assessment. As with any IT risk assessment project a number of high risk items were identified. One item that generated much discussion and rated as one of the highest risk items was the implementation of the CRW system. The system had recently gone into a live production environment at the end of September 2009 and there were a number of issues associated with the implementation which were impacting end users of the system. As a result of the IT risk assessment, a recommendation was made to perform an audit of the system which is the basis for this review.

Overall Conclusions
A total of 10 recommendations were identified during our audit of which two (2) were identified as “high” risk, four (4) were viewed as “moderate” risk with the remaining four (4) deemed “low” risk. Only one of the recommendations related to the “field officer laptops” has a direct impact on the daily functionality of the system. The remaining findings are non-functional in nature and are more controls and recovery focused. Nevertheless, both functional and non-functional controls are important to the overall control environment of the system. An overview of the 10 recommendations has been provided below in the table in section 3.2 while the detailed findings are provided in Appendix 1.

Root Causes
Although some underlying reasons for the identified areas for improvement typically are related to day to day activities competing for resources and priorities such as parallel IT projects, daily system maintenance and support; the additional items that we consider to be the most significant root causes have been highlighted below:

- Limitations of third party product
- Lack of formal documentation in selected project areas

Strengths
In the course of our review we identified the following strengths related to the project implementation efforts associated with the CRW system:

- CCC has knowledgeable and highly committed staff both in ITS and on the business side
- Security administration process is formalized
- Formalized comprehensive IT policies and procedures tied to the COBIT framework
- System utilizes a standardized OS and application platform
- A high performance IBM blade server platform is utilized for the key system servers

Action Plan
Individuals should be given responsibility for creating a formally documented action plan that is properly prioritized. This action plan should utilize the table of areas for improvement in Appendix 1 as a basis for findings to be addressed. The table should be expanded to include a specific person or team responsible for addressing the item along with a target completion date. We suggest that a summary of the report be presented to the executive management together with the proposed action plan. As mentioned in this report a root cause analysis is required to assure that the action plan is including tasks to address issues identified in this report.
# TABLE OF CONTENTS

**EXECUTIVE SUMMARY** .................................................................................................................. 1

**TABLE OF CONTENTS** .................................................................................................................. 2

1 **INTRODUCTION** ......................................................................................................................... 3
   1.1 OVERALL PROJECT DESCRIPTION .................................................................................. 3
   1.2 DESCRIPTION OF SCOPE AND METHODOLOGY .......................................................... 3

2 **OVERVIEW OF CRW PROJECT AND SYSTEMS ENVIRONMENT** .......................................... 5
   2.1 CRW PROJECT ................................................................................................................ 5
   2.2 CRW SYSTEM AND ENVIRONMENT .............................................................................. 5

3 **OVERALL CONCLUSION AND RECOMMENDATIONS** ............................................................ 7
   3.1 OVERALL CONCLUSION ................................................................................................ 7
   3.2 IDENTIFIED AREAS FOR IMPROVEMENT AND RECOMMENDED ACTIONS .................... 9
   3.3 ACTION PLAN .................................................................................................................. 11

**APPENDICES**

Appendix 1: Recommendations
1 INTRODUCTION

1.1 Overall Project Description

Transcendent Group has assisted the City Auditor for the City of Cape Coral ("CCC") in providing information technology audit services by performing a post-implementation review of the City’s CRW / TRAK-iT system. The post-implementation review was performed during August 2010 and was comprised of the following:

- Interviews with key project members, IT support personnel, and significant users on the system.
- Gaining an overall understanding and analysis of key business operations, supporting technology, information flows, and general IT processes.
- Identification of key controls over the CRW application and subsequent assessment of control design effectiveness.
- Identification of gaps in the control environment and quality of mitigating controls, if any.
- Developing recommendations for identified areas for improvement.

During the 4th quarter of 2009 Transcendent Group assisted the City in performing an IT risk assessment. As with any IT risk assessment project a number of high risk items were identified. One item that generated much discussion and rated as one of the highest risk items was the implementation of the CRW system. The system had recently gone into a live production environment at the end of September 2009 and there were a number of issues associated with the implementation which were impacting end users of the system. As a result of the IT risk assessment, a recommendation was made to perform an audit of the system which is the basis for this review.

The report starts with a description of the scope of the project and work performed, followed by a description of the project and the CRW system. In Chapter 3 we provide a conclusion, overview of key findings, and a proposed high level action plan. A detailed description of the identified areas for improvement and suggested actions are provided in appendix 1.

1.2 Description of Scope and Methodology

Due to the complexity of this system and the number of modules within the overall package, the scope of this review was limited to only focusing on the Building Permits and Code Enforcement modules within the system. This high level review included reviewing the following control areas:

- Assess policies and procedures related to the system and related automated processes
- General information technology controls related to assessing:
  - Change management controls
  - Availability controls
  - Incident / problem management effectiveness
  - IT infrastructure for supporting the system, if applicable
- Assess information security controls (access controls)
  - Appropriateness of password management settings
  - Establishment of user roles/groups
  - Appropriateness of system administrators within the system
- Assess controls for critical data interfaces
- Review audit trails / exception reports
• Review logging and monitoring controls
• Disaster recovery and backup management
• Business continuity planning
• Process for the creation of customized reports

We identified and assessed high risk areas and mitigating controls related to the CRW application and conducted a number of interviews with various levels of management and end users. The following main work steps were performed for this review:

• Information gathering of project plan, application and IT environment, and business processes
• High level risk analysis
• Creation and execution of work program
• Assessment of controls related to control objectives
• Discussion and validation of identified risks
• Gap analysis, comparison to best practices and development of suggested actions
• Development of proposed high level action plan to address the identified high risk areas

Identified controls and procedures were reviewed based on defined criteria for sound internal control and management. These criteria are defined in internationally accepted standards such as: ISO 27000-series, COBIT, NIST and PMI. The resulting weaknesses were discussed and validated by key stakeholders and summarized in this report and attached appendix.
2 OVERVIEW OF CRW PROJECT AND SYSTEMS ENVIRONMENT

2.1 CRW Project

The CRW system replaces some of the functionality associated with the H.T.E. system. The RFP for the Community Services system was posted on DemandStar on February 8, 2008 with three vendors selected as finalists. After further analysis the CRW vendor was awarded the contract which was signed on 12/10/2008. Project planning efforts began in January 2009 with both organizations having a separate project manager with respective project team members. The City’s project manager was ITS Director, John Maclean. The receipt of “business process” workbooks and business process reviews between the City and CRW occurred in early 2009 with system acceptance user training and the software installation performed in March and April. End user training was performed in late August through early September with an implementation date of all CRW modules on September 28, 2009. The next planned major upgrade to the system is the Land Management Interface version 2 update with an October 2010 estimated go live date.

2.2 CRW System and Environment

The CRW TRAK-iT version 6.1 is running on a Windows Server 2003 platform with SQL Server 2005 databases. The server infrastructure was initially virtualized using VMware but was later moved to a hardware based IBM blade server platform due to initial performance issues.

The system uses “smart clients” to connect to the TRAK-iT application servers. Remote “field officers’ utilize laptops and Citrix clients to connect to the TRAK-iT database via the internet over air cards. This causes some performance issues due to bandwidth/connectivity issues with the air card connections. Mobile users were initially meant to synchronize the TRAK-iT database to a database on the local hard drive, but this solution could not be utilized due to local database size constraints of the SQL Express database. This would have eliminated performance issues caused by connectivity issues.

The system is currently hosted at multiple data centers. The system’s primary data center is the EOC, which holds the web server, one of the two load balancing application servers, two Citrix servers and the (currently unused) synchronization server. The database server is currently hosted at the city hall data center due to blade chassis space limitations, but is due to be moved to the EOC data center in October 2010. To provide some redundant failover capabilities (with reduced capacity), one of the application servers is located at the Police Department site and two of the Citrix servers are located at the City Hall data center. There is also a virtualized test environment for CRW.

The CRW system has approximately 200 users of the system which are categorized as a user, observer or administrator. Administrators are the most powerful users of the system and the number of these users is very limited. Observers are only provided with inquiry capability within the system while users can be granted a wide range of permissions. Some users have been identified as “power users” of the system in which the number of these users is limited due to the elevated privileges granted to these users. There are some limitations associated with the security functions within the system related to role based security and the ability to easily print security listings. These limitations will be further discussed in the appendix section of this report.
Disaster Recovery (DR) capabilities for the CRW systems are currently a work in progress. The current SunGard contract that provides some DR infrastructure will be discontinued by the end of September 2010. A “warm” DR site will be established at the Ft. Myers/Lee County facility that will provide DR functions for CRW and other critical CCC systems.

A total of four systems interface with CRW. These systems interface with CRW programmatically and to update and/or extract data from the CRW database. The interfacing systems are:

- SunGard OSS Public Safety
- GIS - County data from Lee Property Appraiser
- Active Government Payment & Cashiering POS
- Selectron IVR

An overview of the CRW server environment has been depicted below:
3 OVERALL CONCLUSION AND RECOMMENDATIONS

3.1 Overall Conclusion

Although this audit generated a number of recommendations and there are still outstanding issues being resolved by the vendor, much progress has been made with the system since the implementation in September to the point where a vast majority of the problems have been addressed. It is still important for the City and the vendor to stay committed to resolving the remaining outstanding issues along with the findings generated during this audit. The continued enhancements of the system will provide for a more efficient and better controlled environment for the City while the vendor will have a product for meeting common security standards.

A total of 10 recommendations were identified during our audit of which two (2) were identified as “high” risk, four (4) were viewed as “moderate” risk with the remaining four (4) deemed “low” risk. Only one of the recommendations related to the “field officer laptops” has a direct impact on the daily functionality of the system. The remaining findings are non-functional in nature and are more controls and recovery focused. Nevertheless, both functional and non-functional controls are important to the overall control environment of the system. An overview of the 10 recommendations has been provided below in the table in section 3.2 while the detailed findings are provided in Appendix 1.

Strengths
In the course of our review we identified the following strengths related to the project implementation efforts associated with the CRW system:
- CCC has knowledgeable and highly committed staff both in ITS and on the business side
- Security administration process is formalized
- Formalized comprehensive IT policies and procedures tied to the COBIT framework
- System utilizes a standardized OS and application platform
- A high performance IBM blade server platform is utilized for the key system servers

Key Issues:
The key issues identified during the review are as follows and are described in the following section below:
- Security – Passwords
- Security – Generic User Ids
- Business Continuity Planning
- Disaster Recovery Infrastructure
- Backups
- Field Laptops

Security - Passwords
The password for the user IDs are in clear text in the database which are accessible by certain ITS users granted Administrator capabilities within the system. In addition, many of these passwords are identical which could make it easier for an unauthorized user to gain access to the system with anyone of a number of user IDs. These passwords should be encrypted and a solution should be provided by the vendor.

Security – Generic User Ids
The organization has created some generic IDs in the application that are used by the business for various reasons. Two IDs are shared among approximately five employees for performing “private provider”
functions. The private provider IDs were created for “resulting inspections” and more specifically for instances in which the inspections are performed by private providers and not by City representatives.

Employees in the zoning department assist in performing functions at the zoning counter. They perform a majority of their daily functions with their assigned CRW session at their work desk. Due to the nature of the business, these employees periodically need to leave their area to handle customer requests at the counter. When this occurs it is inefficient for them to sign off their workstation and then sign back onto the workstation at the zoning counter. As a result, a generic user ID was created specifically for employees at the “zoning counter”. This session stays active throughout the day to allow employees to use the session when they are assisting at the counter. Although this is an efficiency convenience, it does not allow for the unique identification of users performing transactions.

**Business Continuity Planning**

Each City department is required to complete a business impact analysis (BIA) which is comprised of a standard template used to obtain critical information about the needs of the business in order to be used as input to assist with recovery efforts during a disaster scenario. Two areas within the BIA request the business to provide downtime procedures and work area requirements in the event the business is required to move operations resulting from a disaster. The DCD’s business impact analysis does not have any procedures or provisions in place related to manual downtime procedures or work area requirements in the event of a disaster. In addition, the business continuity efforts related to the DCD have not been tested.

**Disaster Recovery (DR) Infrastructure**

Due to the CRW database (and SAN) and main backup tape library being located in the same data center, a single catastrophic event in that area can irreversibly destroy one week of CRW data. This is well over the established acceptable RPO (Recovery Point Objective). Now that space has been made available for the server, existing plans to move CRW database server to EOC and store the database data on the EOC SAN should be executed in a timely manner to mitigate this risk.

The DR infrastructure for CRW is work in progress. The current SunGard contract expires by the end of Sept 2010 and will not be renewed. Instead plans are being made for a DR site in Lee County and hardware has been purchased to accommodate DR capabilities for CRW and other systems. The design and technical documentation for this new infrastructure need to be finalized. Also, a DR test plan needs to be established for CRW. DR tests need to be successfully prior to the expiration of the SunGard contract to ensure that DR capabilities have been established.

There is no redundancy for the internet connection at EOC. This is a known single point of failure for CRW remote users. This risk is reduced for field officers if the TRACK-iT synch solution is reinstated as this allows them to work offline from a local database on their laptops, but other remote users e.g. using the shopping cart are still affected by an outage.

**Backups**

No formal backup recovery tests for CRW have been performed and/or documented. To ensure backup recovery capabilities from tape, there is a need to plan and perform a formal CRW backup recovery test from tape, including the database, and to document the test results.

Due to the configuration of server logging and the backup frequency there is a risk that a full audit trails from servers cannot be retrieved from backup tapes. Data may be missing due to log files that are overwritten. Work is currently in progress to address this item.
Field Laptops
With the availability of the just released Rev 2 version of the Microsoft SQL Express database which increases the database size limit to 10 GB from 4 GB, the City plans to reinstate TRAKiT SYNC for all field laptops. TRAKiT SYNC stores the database copy locally on the laptop hard drives, either partially or fully. All field transactions are made against the local database which synchronizes continuously with the main TRAKiT database server in the background. This significantly speeds up transactions in the field, especially in areas with poor air-card coverage. This creates a need to review the sensitivity of all data that are synchronized to the field laptops and determine the needs, if any, for full disk encryption of laptop hard drives to ensure data confidentiality as needed.

Also, due to inherent limitation of database sizes on the laptops, there is a need to analyze and forecast database growth to ensure that the database size limit will not be problem in the foreseeable future. The analysis need to take into account both historical data growth patterns as well as future upgrades or expansion plans for the systems.

Root Causes
Although some underlying reasons for the identified areas for improvement typically are related to day to day activities competing for resources and priorities such as parallel IT projects, daily system maintenance and support; the additional items that we consider to be the most significant root causes have been highlighted below:

- **Limitations of third party product** – Several areas for improvement are related to functional limitations or design technical solutions in the CRW system. Examples include the security administration functionality, password storage for interfaces and the sync solution database size limits.

- **Lack of formal documentation in selected project areas** – The project team has created some formalized system documentation. However, there are some areas such as: backup recovery tests, testing, disaster recovery solution design and testing where solution design, test plans and/or test results, and components of the business continuity plan (and manual downtime procedures) have not been documented. These plans should be formally documented along with specific task lists that need to be completed specifying person responsible, timing, and formal sign-offs, as needed.

3.2 Identified Areas for Improvement and Recommended Actions

This section contains an overview of identified Areas for Improvement. This first section contains the legends to be used in the table below.
Risk Classification / Level

<table>
<thead>
<tr>
<th>Assessment of Significance</th>
<th>Assessment of Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Each area has been risk classified according to the following criteria:

1. **High risk level.** Risk represents a high likelihood and significance to the City. High risk of fraud, security breach, access to or destruction of confidential data, or financial impact to the operations of the City. Very critical to the City’s efficiency and to the fulfillment of the goals of the operation in the short and long-term.
2. **Medium risk level.** Risk represents a moderate level of likelihood and significance to the City. Moderate risk of security breach, access to or destruction of data, or impact to the operations of the City. Critical to a good internal control, efficiency and reliability in the City’s operations.
3. **Low risk level.** Risk represents a lower likelihood and significance to the City. Still essential for a good internal control, efficiency and reliability in the City’s operations.

**Responsible**

The areas of responsibility for each area of improvement have been defined as follows:

- A. City Leadership / City Council
- B. Information Technology Services
- C. System / Business Owners
- D. Vendor

**Investment**

We have estimated the total investment needed to act on the recommendation base on the following scale:

- $ < $3,000
- $$ $3,000-$10,000
- $$$ $10,001-$25,000
- $$$$ > $25,000

The cost is based on an assumed internal cost of $55 per hour and DOES NOT take into account any hardware, software, customization costs associated with addressing the issue.
Priority

For each recommendation we provide the priority level for implementation for each improvement item as a support for the creation of an action plan. The following categories are used:

I Immediate action
II Project to be initiated or completed within 6 months
III Action within 18 months

<table>
<thead>
<tr>
<th>Areas for Improvement</th>
<th>Risk Level</th>
<th>Responsibility</th>
<th>Investment</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security – Passwords</td>
<td>✓</td>
<td>D</td>
<td>$</td>
<td>I</td>
</tr>
<tr>
<td>2. Security Reporting Capabilities and Role Based Security</td>
<td>✓</td>
<td>D</td>
<td>$</td>
<td>III</td>
</tr>
<tr>
<td>4. Business Continuity Planning</td>
<td>✓</td>
<td>B,C</td>
<td>$$$</td>
<td>II</td>
</tr>
<tr>
<td>5. Logging - Exception Reporting and Monitoring</td>
<td>✓</td>
<td>B,C</td>
<td>$</td>
<td>II</td>
</tr>
<tr>
<td>6. Disaster Recovery Infrastructure</td>
<td>✓</td>
<td>B,C</td>
<td>$$$</td>
<td>I</td>
</tr>
<tr>
<td>7. Disaster Recovery Plan</td>
<td>✓</td>
<td>B</td>
<td>$</td>
<td>II</td>
</tr>
<tr>
<td>8. Backups</td>
<td>✓</td>
<td>B,D</td>
<td>$</td>
<td>I</td>
</tr>
<tr>
<td>9. Field Laptops</td>
<td>✓</td>
<td>B</td>
<td>$</td>
<td>II</td>
</tr>
<tr>
<td>10. System Interfaces</td>
<td>✓</td>
<td>B,D</td>
<td>$</td>
<td>II</td>
</tr>
</tbody>
</table>

Each area of improvement is described in Appendix 1.

3.3 Action Plan

Individuals should be given responsibility for creating a formally documented action plan that is properly prioritized. This action plan should utilize the table of areas for improvement in Appendix 1 as a basis for findings to be addressed. The table should be expanded to include a specific person or team responsible for addressing the item along with a target completion date.

We suggest that a summary of the report be presented to the executive management together with the proposed action plan. As mentioned in this report a root cause analysis is required to assure that the action plan is including tasks to address to issues identified in this report.
IDENTIFIED AREAS FOR IMPROVEMENT AND RECOMMENDED ACTIONS

The identified areas of improvement, together with recommended actions in detail are presented below:

Risk classification

<table>
<thead>
<tr>
<th>Assessment of Likelihood</th>
<th>Assessment of Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Each area has been risk classified according to the following criteria:

1. **High risk level.** Risk represents a high likelihood and significance to the City. High risk of fraud, security breach, access to or destruction of confidential data, or financial impact to the operations of the City. Very critical to the City’s efficiency and to the fulfillment of the goals of the operation in the short and long-term.

2. **Medium risk level.** Risk represents a moderate level of likelihood and significance to the City. Moderate risk of security breach, access to or destruction of data, or impact to the operations of the City. Critical to a good internal control, efficiency and reliability in the City’s operations.

3. **Low risk level.** Risk represents a lower likelihood and significance to the City. Still essential for a good internal control, efficiency and reliability in the City’s operations.

Responsibility

The areas of responsibility for each area of improvement have been defined as follows:

A. City Leadership / City Council
B. Information Technology Services
C. System / Business Owners
D. Vendor

Investment

We have estimated the total investment needed to act on the recommendation according to the following scale:

- $ < $3,000
- $$ $3,000-$10,000
- $$$ $10,001-$25,000
The cost is based on an assumed internal cost of $55 per hour and DOES NOT take into account any hardware, software, customization costs associated with addressing the issue.

**Priority**

For each recommendation we provide the suggested priority level for implementation for each improvement item as support for the creation of an action plan. The following categories are used:

| I  | Immediate action |
| II | Project to be initiated or completed within 6 months |
| III | Action within 18 months |

<table>
<thead>
<tr>
<th>Areas for Improvement</th>
<th>Risk Level</th>
<th>Responsibility</th>
<th>Investment</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security – Passwords</td>
<td>✓</td>
<td>D</td>
<td>$</td>
<td>I</td>
</tr>
<tr>
<td>2. Security Reporting Capabilities and Role Based Security</td>
<td>✓</td>
<td>D</td>
<td>$</td>
<td>III</td>
</tr>
<tr>
<td>4. Business Continuity Planning</td>
<td>✓</td>
<td>B,C</td>
<td>$$$</td>
<td>II</td>
</tr>
<tr>
<td>5. Logging - Exception Reporting and Monitoring</td>
<td>✓</td>
<td>B,C</td>
<td>$$</td>
<td>II</td>
</tr>
<tr>
<td>6. Disaster Recovery Infrastructure</td>
<td>✓</td>
<td>B,C</td>
<td>$$$</td>
<td>I</td>
</tr>
<tr>
<td>7. Disaster Recovery Plan</td>
<td>✓</td>
<td>B</td>
<td>$</td>
<td>II</td>
</tr>
<tr>
<td>8. Backups</td>
<td>✓</td>
<td>B,D</td>
<td>$$</td>
<td>I</td>
</tr>
<tr>
<td>9. Field Laptops</td>
<td>✓</td>
<td>B</td>
<td>$$</td>
<td>II</td>
</tr>
<tr>
<td>10. System Interfaces</td>
<td>✓</td>
<td>B,D</td>
<td>$</td>
<td>II</td>
</tr>
</tbody>
</table>

Each area of improvement is described under the relevant reviewed section below.
INDEX RECOMMENDATIONS

A.1  Security - Passwords ................................................................. 4
A.2  Security Reporting Capabilities and Role Based Security .................. 5
A.3  Security - Generic User Ids ....................................................... 6
A.4  Business Continuity Planning ..................................................... 8
A.5  Logging - Exception Reporting and Monitoring ............................. 9
A.6  Disaster Recovery (DR) Infrastructure ....................................... 10
A.7  Disaster Recovery Plan ............................................................. 12
A.8  Backups .................................................................................... 13
A.9  Field Laptops ........................................................................... 14
A.10 System Interfaces ..................................................................... 15
## A.1 Security - Passwords

<table>
<thead>
<tr>
<th><strong>OBSERVATION:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>During our review of application security it was determined that the passwords for the user IDs are in clear text in the database which are accessible by certain ITS users granted Administrator capabilities within the system. In addition, many of these passwords are identical which could make it easier for an unauthorized user to gain access to the system with any one of a number of user IDs. The storage of passwords in clear text is not in compliance with the City’s password policy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>LEVEL OF RISK: HIGH</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RISK:</strong></td>
</tr>
<tr>
<td>Even though access to these passwords is limited to administrators, any user having access to these passwords could sign onto the system as almost any other user making it very difficult to identify the actual user on the system from an audit trail perspective.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>RECOMMENDATION:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>We recommend that the City contact the vendor and formally request the encryption of passwords stored in the application database. The cost associated with enhancements to the system by the vendor is a sensitive topic due to budgetary constraints within the City. Therefore, the City should ask the vendor to absorb any proposed costs as a necessary enhancement to the standard system to mitigate security vulnerabilities and to improve the overall product which should be a general on-going objective of the vendor. Otherwise, this issue along with any other limitations of the system should be brought up at the user conference in order to gain support from other CRW users. In the short-term, while a vendor solution is being discussed or created, the ITS department should change the database passwords that are currently set to the same generic value. Changing the passwords to unique values will make it more difficult for an unauthorized user to gain access to the system with another user ID.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>MANAGEMENT COMMENTS/ACTION PROPOSED:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>We agree and have contacted CRW. CRW has provided a new set-up configuration to allow for encrypting the passwords. This is at no charge. We plan to test this feature during the week of 8/23 with the goal of taking it live by month end.</td>
</tr>
</tbody>
</table>
### A.2 Security Reporting Capabilities and Role Based Security

<table>
<thead>
<tr>
<th>AREA:</th>
<th>OBSESSION:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>During our review of the security within the application it was determined that the system has two weaknesses.</td>
</tr>
</tbody>
</table>

a. The security of the system does not support traditional role based security. Instead, of assigning users to groups with predefined privileges, users are individually assigned specific privileges which makes it more difficult to manage application security and to ensure there is consistency of user privileges. Prior conversations have occurred between the vendor and ITS regarding this topic in which the vendor believes the CRW system supports role based security.

b. The system does not have a user friendly mechanism to generate security reports / listings of the users having access to the core application or the utilities and maintenance application.

The limitations associated with these two items also makes it more difficult for the business to perform their annual security reviews.

<table>
<thead>
<tr>
<th>LEVEL OF RISK: LOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>RISK:</td>
</tr>
<tr>
<td>The establishment and maintenance of security within an application system are key functions for ensuring users are assigned proper privileges. Having tools and reports to manage and monitor security privileges is also important in the daily activities of the security administration function. Without these tools it is difficult for security administration tasks to be performed in a consistent manner and for the business to perform annual reviews of user privileges.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RECOMMENDATION:</th>
</tr>
</thead>
<tbody>
<tr>
<td>We recommend that the City contact the vendor and formally request enhancements to the system to improve the role based security and security reporting features of the system. Role based security was a formal requirement of the system and at this point this requirement has not been fully met.</td>
</tr>
</tbody>
</table>

The cost associated with any enhancements to the system by the vendor is a sensitive topic due to budgetary constraints within the City. Therefore, the City should ask the vendor to absorb any proposed costs as a necessary enhancement to the standard system to mitigate security vulnerabilities and to improve the overall product which should be an on-going objective of the vendor.

<table>
<thead>
<tr>
<th>MANAGEMENT COMMENTS/ACTION PROPOSED:</th>
</tr>
</thead>
<tbody>
<tr>
<td>We agree and have sent a request to CRW to add Role based security as an enhancement to the system and provided a simple specification recommending how we think they should implement this feature. They have added it to their request database.</td>
</tr>
</tbody>
</table>
### A.3 Security - Generic User IDs

**Observation:**

The City’s information security policy (IT-DS5.2-02) requires the use of unique user IDs and passwords which are not to be shared with other individuals. During our review of the CRW application security, it was determined that there are three instances in which user IDs were shared and/or the use of generic user IDs.

1. One user had temporarily lost certain elevated privileges due to a system upgrade. The employee used another user’s ID in order to perform certain high privileged tasks. This issue was fixed during our fieldwork in which the user’s privileges were re-activated.
2. There are two active IDs shared among approximately five employees for performing “private provider” functions. The private provider IDs were created for “resulting inspections” and more specifically for instances in which the inspections are performed by private providers and not by City representatives.
3. Employees in the zoning department assist in performing functions at the zoning counter. They perform a majority of their daily functions with their assigned CRW session at their work desk. Due to the nature of the business, these employees periodically need to leave their area to handle customer requests at the counter. When this occurs it is inefficient for them to sign off their workstation and then sign back on to the workstation at the zoning counter. As a result, a generic user ID was created specifically for employees at the “zoning counter.” This session stays active throughout the day to allow employees to use the session when they are assisting at the counter. Although this is an efficiency convenience, it does not allow for the unique identification of users performing transactions.

**Level of Risk:** **Moderate**

**Risk:**

The use of generic user IDs and the sharing of user IDs are not in compliance with the City’s information security policy. In addition, these practices significantly limit the City’s ability to know the individual using the ID to perform tasks on the system. If unauthorized tasks are performed, it would be very difficult to know the identity of the person performing the transactions.

**Recommendation:**

Although observation #1 has been addressed, the ITS department should modify internal procedures so that whenever upgrades are performed in the future there is assurance that all users privileges are properly restored.

In addition, we recommend that the ITS department and the business meet to discuss options for most appropriately addressing observations #2 and #3. Ideally, the use of shared, generic user IDs would not exist with each user of the system being assigned unique user IDs and passwords which uniquely identifies them and allows for proper tracking of activities.

With regards to item #2, one option could entail assigning each user their own “private provider” user ID to allow for the proper tracking of users’ activities within the system. A similar solution should be created for observation #3 where unique ID’s are assigned or user’s being required to sign-off their workstation and re-sign-on as the zoning counter. However, if the organization chooses not to implement an appropriate solution and decides to continue the use of the shared user IDs, then as part of the exception process, formal documentation should be performed outlining management’s acceptance of the risk and exception to the information security policy.
Agreed: Regarding point 1: the root cause was that ITS had a procedure to manually delete and re-add the elevated privileges users as part of the version upgrade process and missed re-adding one of them following a particular upgrade. An SQL script has now been developed to automate deletion & re-addition which will resolve the issue. Regarding Point 2: we will add individual private provider user IDs for each of the five employees thus resolving this issue. Regarding Point 3: DCD will change operational procedures to assign a specific individual to cover the zoning counter. These users will then sign on with their normal ids as will anyone designated to cover them during lunch periods, etc.
A.4 Business Continuity Planning

<table>
<thead>
<tr>
<th>AREA:</th>
<th>LEVEL OF RISK: MODERATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBSERVATION:</td>
<td>RISK:</td>
</tr>
<tr>
<td>From a business continuity perspective the City has a number of plans in place: the continuity of operations plan (COOP), a business continuity plan, a disaster recovery plan and a business impact analysis (BIA) for every department. The goal is for the various plans to be integrated in order to provide a comprehensive continuity of operations solution for all aspects of the City’s life safety, business and information technology recovery efforts.</td>
<td>The formal documentation and testing of business continuity plans (and downtime procedures) serve an important function for any organization during the recovery efforts of a small or large disaster. Without the formalization and testing of these plans and procedures, it will be difficult to know if the organization will be properly prepared for a disaster event. Recovery times could be significantly increased if the plan is not fully documented and tested.</td>
</tr>
</tbody>
</table>

We have reviewed the above mentioned plans as they relate to the CRW system and the Department of Community Development (DCD). On an annual basis every City department is expected to perform an update and review of the BIA which feeds the business continuity and disaster recovery plans. During our review of the DCD’s BIA the following areas of improvement were noted:

- The “manual procedures / business recovery” section of the document has not been completed which essentially means there are no formally documented downtime procedures for the department related to the CRW system

- The “work area requirements” section of the document has not been completed

- No testing of the plan has been performed

RECOMMENDATION:

We recommend that the BIA for the DCD be reviewed and updated to address the manual procedures and work area requirements sections of the document that have not been completed by the business. In addition, a review process should be incorporated to ensure all BIA’s are completed within the expected timeframes (i.e. annual basis) and all sections are properly completed.

Finally, once these tasks have been completed, the City should create a strategy for testing the business continuity plans. This testing could start by having each department test various components of the manual downtime procedures which could include table top exercise. The testing efforts should then continue to expand by testing business continuity plans and then a more comprehensive integrated test of the business continuity and disaster recovery plans. Results of these tests should be formally documented to serve as a basis for continued improvements to the plans.

MANAGEMENT COMMENTS/ACTION PROPOSED:

1. DCD to complete the addition of the manual procedures into the DCD BIA by 8/31/2010.
2. ITS will develop a plan to test the BCP/DR plans following hurricane season in the December-January time-frame.
### A.5 Logging - Exception Reporting and Monitoring

<table>
<thead>
<tr>
<th>AREA:</th>
<th>LEVEL OF RISK: LOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBSERVATION:</td>
<td>RISK:</td>
</tr>
<tr>
<td>The topic of audit logs and exception reporting is a priority area for the City and was included as a requirement of the system. During the RFP process the vendor stated that the CRW application did in fact have comprehensive logging. However, after the system had been selected and during the testing phase of the system it was determined that the only log history provided with the system was for fees. This deficiency was communicated to the vendor and was subsequently addressed. Although logging of application and server transactional activity is in place, there are essentially no reports in place to summarize and print critical transactional activity or for the generation of exception reports to automatically notify the business and/or ITS of system conditions and changes to critical system parameters, data or configurations at the application or server level.</td>
<td>The important task that has been completed was the implementation of logging capabilities within the system. Even though logging exists, it is difficult for the end users to access the logs in the event of a problem or questionable without involvement from ITS. The creation of audit log reports and exception reports enables the business to monitor activities of the system without dependence on ITS.</td>
</tr>
</tbody>
</table>

| MANAGEMENT COMMENTS/ACTION PROPOSED: |
| Bryon Maine will augment with audit trails for ProjectTRAK in September and will continue on a module by module basis until complete. Additionally, Fidel Deforte has contacted Microsoft to set up a mechanism for archiving and copying all “Event Viewer Logs” from the production servers to a “Storage Server” for monitoring and audit purposes. |

- Bryon Maine will augment with audit trails for ProjectTRAK in September and will continue on a module by module basis until complete. Additionally, Fidel Deforte has contacted Microsoft to set up a mechanism for archiving and copying all “Event Viewer Logs” from the production servers to a “Storage Server” for monitoring and audit purposes.
A.6 Disaster Recovery (DR) Infrastructure

**OBSERVATION:**

The City utilizes three data centers to host IT infrastructure: EOC is the main data center, City Hall is the "original" data center slowly being phased out and the Police Department (PD) will serve as a temporary failover site for CRW. The three data centers are connected with 10Gb fiber. The EOC is the intended main CRW data center. The DR infrastructure for CRW is currently a work in progress and currently just one server is located at PD for redundancy purposes (one of two application servers). The current Sungard contract for DR infrastructure provisioning is expiring by the end of September 2010 and will not be renewed. Instead, a new DR "warm site" will be set up at the Lee County Clerk of Courts (LCCoC) data center in Fort Myers. A newly acquired IBM blade chassis will provide 6 blade servers and 12 terabytes of storage running for multiple systems. The following issues have been identified with the current DR infrastructure:

1. The CRW database server currently resides at City Hall and the data is stored on the City Hall SAN. This was due to lack of space in the EOC blade chassis at the time of live system deployment. Additional blade chassis space have since been provided and there are plans to move the database server to EOC.
2. A single internet connection at the EOC is shared by all three data centers. This is a known single point of failure.
3. Each data center has separate SANs. There are plans to replicate data between the three SANs to increase data redundancy.
4. No system documentation describing the proposed DR infrastructure has been identified.
5. No DR tests have been performed relating to the current Sungard contract. No DR test plans are currently documented for the new proposed DR infrastructure.

**LEVEL OF RISK: HIGH**

**RISK:**

1. Risk of data loss. A single catastrophic event (e.g. a fire) can destroy both the data on the SANs and up to one week of historic data as the last week of backup tapes are not available elsewhere. This is a high risk item.
2. Single point of failure. Risk of system unavailability for mobile users.
3. Reduced dependency on backup tapes and increases data redundancy.
4. Risk of reduced/insufficient disaster recovery capabilities
5. Risk of reduced/insufficient disaster recovery capabilities

**RECOMMENDATION:**

We recommend the following related to the DR infrastructure:

1. Move the CRW database server to the EOC as planned and store the database data on the EOC SAN.
2. Consider establishing redundant internet connectivity.
3. Establish data replication between the three SANs as planned. This will increase data redundancy and mitigate some risks associated with recommendation #1 above.
4. Finalize the design and technical system documentation for the CRW DR infrastructure planned for the LCCoC DR site.
5. Establish a DR test plan for CRW, either on its own or as part of existing DR test plans. Execute the tests according to established plans and document the test results. DR tests need to be successfully performed prior to the expiration of the SunGard contract to ensure that expected DR capabilities have been established.
MANAGEMENT COMMENTS/ACTION PROPOSED:

1. The CRW database server is now being mirrored to the EOC SAN - Timing is 11/30/2010
2. We will obtain costs for redundant internet connectivity – which would also be required as part of any Cloud computing initiatives.
4. The design will be completed by 9/30/2010. By that date we will also have an agreement with LCCoC on the new DR site.
5. We are updating the design from the current plan with SunGard. The current plan requires restoring systems from tapes. The new design that will be documented by 9/30/2010 will specify a redundant host server at the LCCoC sites that will be online and having data copied on a regular timeframe, in addition to having the tape option. This will add higher availability to what was offered by SunGard. We will test tape recovery by 12/31/2010.
### A.7 Disaster Recovery Plan

<table>
<thead>
<tr>
<th>AREA:</th>
<th>LEVEL OF RISK: LOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBSERVATION:</td>
<td>RISK:</td>
</tr>
<tr>
<td>The Disaster Recovery (DR) plan, IT-DS4.8-01 City of Cape Coral Information Technology DR Plan.docx, have been updated with information relating to CRW but the following areas of improvement were noted:</td>
<td>Risk of reduced disaster recovery capabilities and/or delays in executing recovery plans.</td>
</tr>
<tr>
<td>1a. No backup information for CRW is provided under section 2.3, page 24.</td>
<td></td>
</tr>
<tr>
<td>1b. CRW is listed only under the City Hall Data Center on page 42 but prioritized under EOC Data center on page 44 and PDHQ on page 45.</td>
<td></td>
</tr>
<tr>
<td>1c. CRW is not prioritized in the hurricane scenario, section 3.3.4 page 52.</td>
<td></td>
</tr>
<tr>
<td>MANAGEMENT COMMENTS/ACTION PROPOSED:</td>
<td>RECOMMENDATION:</td>
</tr>
<tr>
<td>Completed. IT-DS4.8-01 updated 8/20/2010</td>
<td>We recommend the following relating to Disaster Recovery planning.</td>
</tr>
<tr>
<td></td>
<td>1. Update the following sections in the City of Cape Coral Information Technology DR Plan:</td>
</tr>
<tr>
<td></td>
<td>a. Add CRW information describing frequency, timing and location of backups in section 2.3.</td>
</tr>
<tr>
<td></td>
<td>b. Update sections 3.1.2 – 3.1.5 to accurately reflect the current CRW infrastructure.</td>
</tr>
<tr>
<td></td>
<td>c. Add CRW to the hurricane scenario recovery priorities, section 3.3.4, as applicable.</td>
</tr>
</tbody>
</table>
## A.8 Backups

<table>
<thead>
<tr>
<th>AREA:</th>
<th>LEVEL OF RISK: MODERATE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OBSERVATION:</strong></td>
<td><strong>RISK:</strong></td>
</tr>
<tr>
<td>The following areas of improvement were noted with the current backup efforts:</td>
<td>Risk of data loss and system unavailability.</td>
</tr>
<tr>
<td></td>
<td>Risk of missing audit trails in Windows server logs.</td>
</tr>
<tr>
<td>1. While some file recovery tests and database restores to test environments have been performed, no formal full backup recovery tests for CRW (especially from tape) have been performed and documented.</td>
<td><strong>RECOMMENDATION:</strong></td>
</tr>
<tr>
<td>2. Windows and database logs are only stored on the local machines. All windows logs store 18MB before being overwritten. Work is in progress to automatically store logs in dedicated off-site storage.</td>
<td>We recommend the following relating to CRW backups:</td>
</tr>
</tbody>
</table>

| MANAGEMENT COMMENTS/ACTION PROPOSED: | 1. Plan and perform a formal CRW backup recovery test from tape, including the database, and document the test results. |
| | 2. Review and assess the current CRW log retention capabilities on backups. Consider CRW application logs, server and database Windows event logs, application logs and security logs. Adjust log settings, and management and backup policies to meet established business requirements and needs. |

| 1. Will be done in the December 2010 – January 2011 time-frame in conjunction with the test of the BCP/DR plans. |
| 2. Will review & develop solution by end of calendar year 2010. |
A.9 Field Laptops

**AREA:**

**OBSERVATION:**
Field officers use laptops with air cards to connect to CRW remotely. The original solution used the TRAK-iT Sync solution to download the CRW database to local hard drives allowing both online and offline access to the system. This database, if fully synchronized to a laptop, is likely to contain some sensitive data e.g. Officer’s names. In addition, the laptops are not encrypted.

The original SQL Server Express database solution had a 4 GB size limit that prevented the use of that solution. A Citrix implementation that provides online access only; therefore, replaced the TRAK-iT Sync solution, but that solution suffers from performance and/or availability issues due to limited air card coverage/bandwidth.

There are now plans to revert to the TRAK-iT Sync solution since a new version of the database increases the database size limit to 10 GB.

**LEVEL OF RISK: MODERATE**

**RISK:**
1. Risk of unauthorized access to sensitive data on lost/stolen laptops. There is a risk of negative publicity if it is publicly known that an unencrypted laptop with sensitive data is lost, even though unauthorized access to said data is not confirmed or easily accomplished.
2. Risk of scalability constraints with client laptops.

**RECOMMENDATION:**

We recommend the following related to the field laptops:

1. Review the sensitivity of all data that are synchronized to the field laptops and determine the needs, if any, for full disk encryption of laptop hard drives to ensure data confidentiality as needed.
2. Analyze and forecast database growth to ensure that the SQL Server Express database size limit will not be problem in the foreseeable future. If so, re-evaluate and redesign the proposed solution as needed. The analysis needs to take into account both historical data growth patterns as well as future upgrades or expansion plans for the systems by the business and ITS.

**MANAGEMENT COMMENTS/ACTION PROPOSED:**

1. DCD would prefer that sensitive data stored on laptops via TRAKiT SYNC be encrypted. Prior to installing SYNC into production, ITS is evaluating options for full disk encryption including open source products and, of course, will test SYNC with disk encryption to ensure there are no adverse performance issues.
2. At the current rate of database growth we are adding 0.5 GB per year. At this rate we should be clear for 10 years given that the new SQL Express DB provides 6 GB more than we currently store.
**Area:**

**Observation:**

The Active Government Payment & Cashiering POS interface utilizes the “TRAKiT” user to access the database. The password is hardcoded (compiled) into the `ClassAccountingInterface.exe` executable file. A knowledgeable attacker may be able to extract the password from the application. Also, vendor developers may have access to the password. The password itself is not known. If a weak password is used it may be susceptible to brute force attacks.

The IVR interface also uses CRW user name and password to connect to the database. It is unclear how that password is stored and who has access to it.

<table>
<thead>
<tr>
<th>Level of Risk: Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk: Risk of unauthorized access to the CRW database and data.</td>
</tr>
</tbody>
</table>

**Recommendation:**

Review CRW username/password usage and storage for all CRW interfaces and contact the affected vendor(s) to ensure the following:

- If the password is not known, request the password from the vendor
- Ensure that the password used is sufficiently complex
- Ensure that access is sufficiently restricted to file areas that contain non-encrypted passwords either in executable files or regular files e.g. configuration files.
- Ensure that vendor knowledge about, and access to, CRW passwords is kept to a minimum and on a need to know basis only.

**Management Comments/Action Proposed:**

CRW agrees that for the “old” VB API that Active Government is using that the password is embedded in the `ClassAccountingInterface.exe` file. However they think that very sophisticated programming indeed would be required to access this password and question whether it would be possible. When Active Government transitions to the new CRW dotnet interface - which they are currently working on - the username/password will need to be divulged separately to Active Government by the City in order for Active to pass via the API. Selectron already uses the dotnet API. We verified that the password is strong.