Richmond City Council

The Voice of the People. *Richmond, Virginia*

OFFICE OF THE CITY AUDITOR

REPORT # 2010-06
AUDIT
of the

Department of Public Utilities
Customer Information System (BANNER)

January 2010

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

City of Richmond
City Auditor

Executive Summary

January 12, 2010

The Honorable Members of Richmond City Council
The Richmond City Audit Committee
Mr. Byron C. Marshall, CAO

Subject: Department of Public Utilities
Customer Information System (BANNER) Audit

The City Auditor's Office has completed an audit of the Department of Public Utilities (DPU) BANNER Customer Information System (CIS). This audit covers general controls (access to programs and data, program changes and backup and recovery) and application controls during the 13-month period ended July 31, 2009. This audit was conducted in accordance with Generally Accepted Government Auditing Standards promulgated by the Comptroller General of the United States and COBIT guidelines issued by ISACA

Salient Findings:

- Business continuity planning (BCP) is a critical, logistical plan for partial or complete recovery of mission-critical systems, processes or environments interrupted due to a disaster, within a predetermined time. It includes a business impact analysis to develop strategies for minimizing risk and identifying the impact of disruptions. DPU has completed a business impact analysis but has not finalized a BCP. The department is working with the City's Emergency Management office to develop and implement a BCP. The department will need assistance from the Department of Information Technology in this endeavor.

- Without a finalized BCP, DPU may not be able to perform a partial or complete recovery of mission-critical systems, processes or environments, within a predetermined timeframe. Disaster strikes without warning. Many times, the organization does not have time to plan or react. A plan is essential for an organization to restore and continue critical processes for an organization to resume business. Therefore, expedient completion of the BCP is critical for the City of Richmond.

- Allowing access to the root account on the operating system for this application could be misused. Currently, the users with knowledge of the root (administrator) password can log in and perform the following administrator functions without proper accountability:
  - Modify system logs;
  - Apply operating system updates, patches, and configuration changes;
  - Install new hardware and software; and
  - Add, remove, or update user account information, reset passwords, etc.

  The above situation is undesirable and can be misused without timely detection.

- DPU's password policy does not comply with the City's password policy and needs improvement.

The City Auditor's Office appreciates the cooperation of the staff of the Department of Public Utilities during this audit. A written response to the report with an action plan and target dates for implementation has been received and is included with this report. Please contact the City Auditor's Office if you have any questions or comments.

Umesh Dalal, CPA, CIA, CIG
City Auditor

900 East Broad Street, Room 806 * Richmond, VA 23219 * 804.646-5616 * Fax 804.646.2230 * www.richmondgov.com

#	*COMPREHENSIVE LIST OF RECOMMENDATIONS*	*PAGE*
1	**Continue to work with Emergency Management and DIT to finalize the Business Continuity Plan in accordance with generally accepted practices such as the COBIT framework and FEMA guidelines to reduce the impact of a major disruption on key business functions and processes.**	**6**
2	**After finalizing the Business Continuity Plan, test the BCP on a regular basis.**	**6**
3	**Provide all staff with regular continuity planning training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the test results.**	**6**
4	**Restrict users from direct log in to the root account.**	**8**
5	**Limit the administrator access to only a few individuals, preferably two or three users, who require such access to perform their job roles.**	**8**
6	**Establish a formal written termination policy and communicate the termination policy to appropriate staff.**	**10**
7	**Once the policy is established, enforce the procedures related to removing separated user access within the network and CIS, including the removal of system access for all separated employees.**	**10**
8	**Establish the password minimum length setting for CIS and the PAUL server in accordance with the City User Password policy.**	**11**
9	**Enable the password history setting on the PAUL server to prevent users from reusing the same password each time it is changed.**	**11**
10	**Activate password settings for the Oracle user profiles in accordance with the City User Password policy.**	**11**

Introduction, Objective, Methodology & Background

Introduction

The City Auditor's Office has completed an audit of the Department of Public Utilities (DPU) BANNER Customer Information System (CIS). This audit covers general controls (access to programs and data, program changes and backup and recovery) and application controls during the 13-month period ended July 31, 2009.

This audit was conducted in accordance with Generally Accepted Government Auditing Standards promulgated by the Comptroller General of the United States and Control Objectives for Information and related Technology (COBIT) guidelines issued by Information Systems Audit and Control Association (ISACA). Those standards provide a reasonable basis for the conclusions regarding the internal control structure over the BANNER system and the recommendations presented.

Audit Objective

Overall objectives of the audit were to:

- Determine whether adequate Information Technology (IT) general controls for access to programs and data, program changes and computer operations had been established by management; and
- Evaluate the adequacy and functionality of CIS (BANNER) and related IT controls and practices.

Methodology

To complete this audit, the auditor performed the following procedures:

- Interviewed staff and management;

- Performed risk analysis associated with each of the control objectives;
- Reviewed and evaluated policies and procedures;
- Performed inquiry, inspection and observation procedures and tested the system controls; and
- Performed other audit procedures as deemed necessary.

Background

To support their daily operations, DPU purchased the BANNER Customer Information System (CIS) and heavily customized it to adapt to their needs. CIS is critical to DPU as it provides automated capabilities to collect, manage, and analyze information about customers, locations, accounts, and the provision of services. It specifically supports DPU operations such as electric, gas, water, wastewater, and storm water. CIS processing is controlled through the use of rules and validations, which allows DPU to select options which fit its business requirements and policies. CIS maintains the utility's accounts receivable, and retains histories such as service, credit, billing, account summaries, and audit trails. CIS includes processes to calculate charges, print bills, process delinquent charges, and apply and distribute payments.

BANNER (CIS) is a critical computer system for multiple utilities

DPU is responsible for the day-to-day management of CIS, including application administration, administering the infrastructure supporting the application, development activities, application security, managing changes, computer operations, and end-user support.

The table below depicts the revenues generated and the average number of customers processed in CIS for fiscal year 2009, by utility:

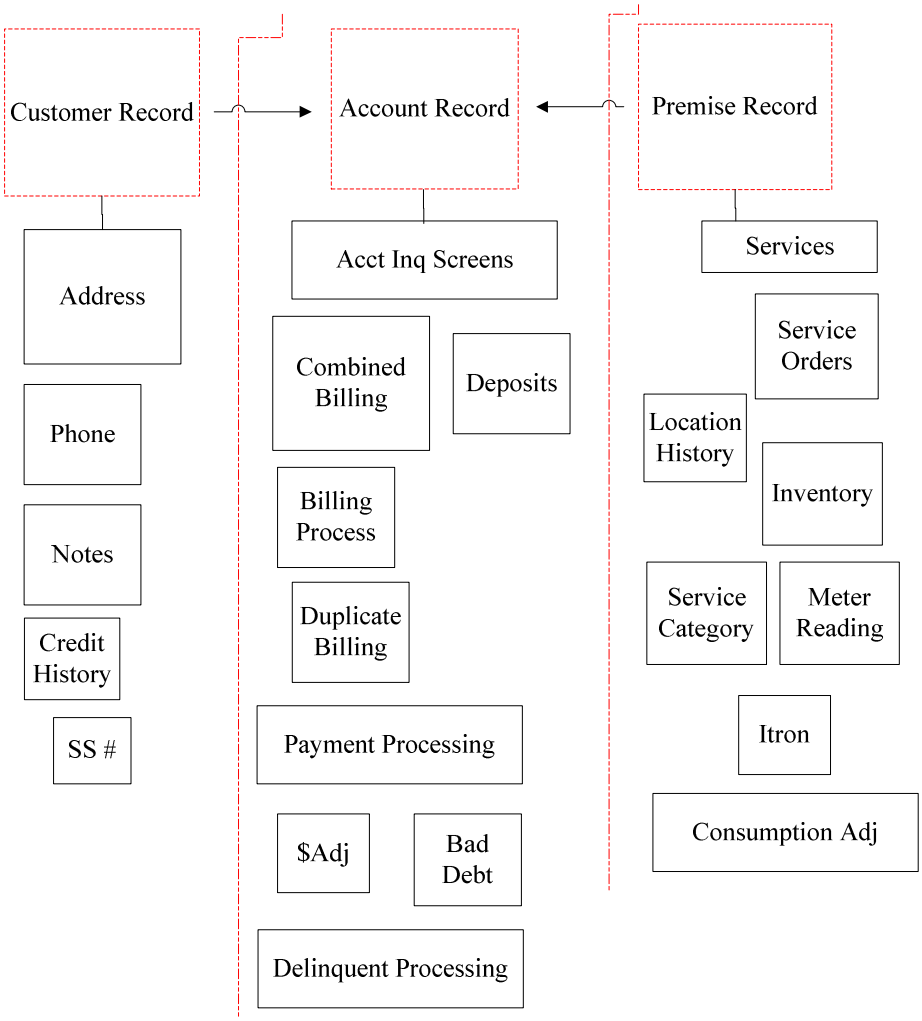
Utility	Avg. # Customers	Revenue
Gas	108,784	$226,839,087
Water	61,879	$54,004,082
Wastewater	58,772	$58,799,316

Source: DPU

Note: There was no billing for storm water in fiscal year 2009. The storm water fee became effective in July 2009.

System Overview

The flowchart below depicts the overall functionality of CIS:



Observations and Recommendations

Business Continuity Plan

Business continuity planning (BCP) is a critical, logistical plan for partial or complete recovery of mission-critical systems, processes or environments interrupted due to a disaster, within a predetermined time. It includes a business impact analysis to develop strategies for minimizing risk and identifying the impact of disruptions. Generally accepted best practices, COBIT, recommend that IT continuity plans be designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding and potential business impacts and address requirements for resilience and alternative processing of all critical IT services. It should also cover usage guidelines, roles and responsibilities, procedures, and communication processes.

A BCP is designed to reduce the impact of a major disruption on the organization

DPU has performed a business impact analysis and documented a BCP for their operations and mission critical systems. However, the BCP is still in a draft format and has not been finalized. According to management, DPU is working with the City Emergency Management Office to revise the BCP into the new format to standardize the plan across different agencies. The BCP will be updated to include the essential functions and interdependencies between different agencies/systems. This is a citywide process and all city agency business continuity plans will remain in draft form until this process is completed. The draft plan includes the following key components as recommended by COBIT best practices:

DPU has performed a business impact analysis but they have not finalized the BCP

- Prioritization of processes and applications with respect to timeliness of recovery and return;

- Roles and responsibilities of the IT function, vendors providing recovery services, users of services and support administrative personnel;
- Listing of system resources requiring alternatives; and
- Testing schedules.

DPU management during their walkthrough noted that the plan needs to be updated with the following:

- Key individuals and their backups need to be identified for all critical functions identified in the plan;
- Alternate facility operations need to be identified and documented; and
- Operational Procedures and Go-Kits (vital records and documents, special equipment) for the alternate facility need to be documented.

DPU is working with the City's Emergency Management office to test and finalize the BCP

Also, the BCP has not been tested as it is still a draft. Generally accepted best practices, COBIT and the Federal Emergency Management Agency (FEMA) recommend:

- Quarterly testing of alert, notification, and activation procedures;
- Quarterly testing of emergency communications systems capabilities;
- Semiannual testing of plans for the recovery of vital records, databases, critical information systems, services, and data at primary and alternate facilities;

- Annual testing of primary and backup infrastructure systems and services at alternate work sites;
- Semiannual tabletop exercise (can be waived if occurs during a functional exercise or full scale exercise year); and
- Full-scale exercise to be performed every five years.

Having a final, properly tested BCP for the BANNER system is critical

Without a finalized BCP, DPU may not be able to perform a partial or complete recovery of mission-critical systems, processes or environments, within a predetermined timeframe. Disaster strikes without warning. Many times, the organization does not have time to plan or react. A plan is essential for an organization to restore and continue critical processes to resume business. Therefore, expedient completion of the BCP is critical for the City of Richmond.

Recommendations:

1. ***Continue to work with Emergency Management and DIT to finalize the Business Continuity Plan in accordance with generally accepted practices such as the COBIT framework and FEMA guidelines to reduce the impact of a major disruption on key business functions and processes.***

2. ***After finalizing the Business Continuity Plan, test the BCP on a regular basis.***

3. ***Provide all staff with regular continuity planning training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the test results.***

Access to the Admin (root) Account

On the operating system (Unix) for BANNER software, "root" is a special account used for system administration. Users with access to root have privileges such as user administration, changing passwords, and ownership of files. Regular users do not have the same level of access to perform similar functions. Users with the knowledge of the root account password can log in using this account and perform actions without any user accountability. It is impossible to trace an act of misconduct based on who logged into the computer as the password is shared by all the system administrators. To ensure accountability, it is common practice to deny users' direct login to the root account by utilizing a "switch user" utility. This requires the user to log in with the user's personal login ID and password. The utility then grants the user access to the root account, retaining the audit trail. Currently, the "switch user" utility is not implemented on the Unix server supporting CIS. Therefore, users with knowledge of the root password can log in and perform the following administrator functions without proper accountability:

Allowing access to root accounts on the operating system could be misused

- Modify system logs;
- Apply operating system updates, patches, and configuration changes;
- Install new hardware and software; and
- Add, remove, or update user account information, reset passwords, etc.

The above situation is undesirable and can be misused without timely detection.

Recommendation:

4. ***Restrict users from direct log in to the root account.***

System Administrator Privileges

As described, the system administrators have high level access within the application. As recommended by COBIT, user access should be based on "least privilege" and "need-to-know" so that users have adequate access that is specifically and legitimately required for performing their assigned job duties. This procedure would ensure system security to safeguard information against unauthorized use, disclosure, modification, damage or loss.

DPU inadvertently granted administrator access to multiple users; this error has been properly addressed

Administrator access should be restricted to the fewest number of individuals that require this access based on their job responsibilities. During the audit, it was noted that 58 user accounts had administrator access privileges to CIS. In July 2009, DPU implemented the storm water billing module. During this process, 50 users were inadvertently granted administrator access in error. This error was identified as part of DPU's internal user access review process and has been corrected.

Recommendation:

5. ***Limit the administrator access to only a few individuals, preferably two or three users, who require such access to perform their job roles.***

Internal Controls

According to Government Auditing Standards, internal control, in the broadest sense, encompasses the agency's plan, policies, procedures, methods, and processes adopted by management to meet its mission, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It

also includes systems for measuring, reporting, and monitoring program performance.

Generally, internal controls were found to be adequate

Based on the results and findings of the audit methodology employed, auditors concluded that internal controls relevant to CIS are adequate and functioning effectively. However, the auditor noted several control deficiencies in the following areas:

Terminated employees retained access to CIS

DPU does not have a formal policy or procedure for removing or disabling access to CIS and supporting systems. During the audit, it was noted that two terminated employees during fiscal year 2009 retained access to CIS. Also, three terminated employees that separated from DPU had active accounts on the Oracle database supporting CIS. Generally accepted best practices, COBIT, recommend "Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending, and closing of user accounts." When termination policies and procedures are not present and therefore not communicated to all stakeholders, the chance of terminated users having active user accounts increases. Such a situation is referred to as "an orphan account."

Allowing terminated employees to retain access to the system could result in misuse

There is an increased risk that having "orphan accounts" may allow:

- Unauthorized changes to the data or customer accounts by a separated user;
- Confidential data theft by a separated user; or
- Unauthorized access to the system by active employees or hackers using the "orphan accounts" without an audit trail.

When termination policies are missing or not communicated, DPU cannot enforce the procedures to either disable or delete access upon a user's separation, potentially limiting DPU's recourse for failing to abide by the established policies.

Recommendations:

6. ***Establish a formal written termination policy and communicate the termination policy to appropriate staff.***
7. ***Once the policy is established, enforce the procedures related to removing separated user access within the network and CIS, including the removal of system access for all separated employees.***

Non-compliance with policy

The City User Password policy requires a minimum password length of eight characters. However the minimum password length for CIS and the PAUL (CIS Unix production server) is set to six characters which does not comply with the minimum password length requirement set forth in the City User Password policy.

The password policy for CIS needs improvement

Additionally, the City User Password policy requires the user account revocation to be set to 60 days. However the user account revocation on the PAUL server is set to 180 days which does not comply with the City User Password policy. Also, the password history is not enforced on the PAUL server. As a result, users may reuse the same password each time it is changed. The password settings for length, expiration, lockout, and complexity are not set up in the profiles for the Oracle database that supports CIS. Default values are being used.

COBIT recommends that a password policy include:

- Enforcing initial password change on first use;
- Requiring an appropriate minimum password length;
- Establishing an appropriate and enforced frequency of password changes;
- Checking the password against list of not allowed values;
- Protecting emergency passwords; and
- Suspending a user ID after five repeated unsuccessful log on attempts.

Failure to maintain strong password settings increases the risk that individuals can gain unauthorized access to the application and make inappropriate changes to data.

Recommendations:

8. ***Establish the password minimum length setting for CIS and the PAUL server in accordance with the City User Password policy.***
9. ***Enable the password history setting on the PAUL server to prevent users from reusing the same password each time it is changed.***
10. ***Activate password settings for the Oracle user profiles in accordance with the City User Password policy.***

MANAGEMENT RESPONSE FORM

DPU - CUSTOMER INFORMATION SYSTEM (BANNER) AUDIT

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
1	*Continue to work with Emergency Management and DIT to finalize the Business Continuity Plan in accordance with generally accepted practices such as the COBIT framework and FEMA guidelines to reduce the impact of a major disruption on key business functions and processes.*	Y	As noted by the auditor, the development of the DPU COOP Plan is in process and substantial progress has been made on this project. DPU hired a Project Management Analyst specifically to work on this project. The employee is tasked with coordinating the completion of the department plan and ensuring its compatibility with the comprehensive city plan. The DPU plan will be finalized once it has been incorporated into the city's COOP Plan through the Department of Emergency Management. DPU will complete its initial portion of this process (completion of the draft COOP Plan and desired DIT recovery time periods) by June 30, 2010.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Deputy Director II		6/30/2010 for DPU Portion ONLY
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
2	*After finalizing the Business Continuity Plan, test the BCP on a regular basis.*	Y	The testing and training on the DPU COOP Plan on a regular basis is already detailed in the draft COOP Plan in the Section entitled COOP Administration and Support. DPU will follow this plan to ensure that compliance with all aspects of the plan, which include testing and training, will be done on a regular basis. Listed training and testing will be implemented along with existing emergency training and testing.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Deputy Director II		6/30/11
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
#	**RECOMMENDATION**	**CONCUR Y-N**	**ACTION STEPS**
3	*Provide all staff with regular continuity planning training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the test results.*	Y	The testing and training on the DPU COOP Plan on a regular basis is detailed in the draft COOP Plan in the Section entitled COOP Administration and Support. Currently DPU regularly tests and trains on its emergency preparedness and Incident Command System (ICS) responses. Once the COOP Plan is finalized, listed training and testing will be implemented along with existing emergency training and testing.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Deputy Director II		6/30/11
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
4	*Restrict users from direct log in to the root account.*	Y	Log in procedures have been changed to prevent logging into the root account. Customer data was never at risk prior to this change because, in order to log into the root account, an individual must have first logged into the City's network and have access to the root account. In order that we track changes, administrators must now log in with their unique CIS user ID and then switch to the root account so that changes made can be tracked by individual administrator.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Business Analysis Manager		
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
			Completed December 2009

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
5	*Limit the administrator access to only a few individuals, preferably two or three users, who require such access to perform their job roles.*	Y	Administrator access has been limited to a minimum number of employees in DPU's MIS division who require that level of access to perform their job functions. In addition, random audits are being performed to determine the appropriateness of user accounts and permissions granted.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Business Analysis Manager		
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
			Completed December 2009.

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
6	*Establish a formal written termination policy and communicate the termination policy to appropriate staff.*	Y	A termination policy has been drafted and is currently being reviewed by MIS and DIT. At its core, the policy establishes a procedure whereby DPU terminations and transfers will be communicated to CIS administrators on a real time basis. Administrators will determine if the employee had access to CIS and if so inactivate the employee's account. This procedure is supplemented by the current policy of revoking access to the City's network once an individual is no longer employed by the City. Customer data was and is not at risk because CIS is a secondary system within the City's network and an individual must first log into the network before they can access the CIS system. Without network access, it is not possible to enter the CIS system.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Business Analysis Manager		2/1/10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
7	*Once the policy is established, enforce the procedures related to removing separated user access within the network and CIS, including the removal of system access for all separated employees.*	Y	Beginning in October 2009, DPU began a quarterly review process of inactive accounts. A report is generated highlighting accounts that have not been accessed in the preceding 90 days and those accounts are reviewed to determine if access to CIS is required. Accounts that are no longer needed will be inactivated. This audit procedure will act as a safety net to ensure that accounts of separated users are removed.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		2/1/10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
8	*Establish the password minimum length setting for CIS and the PAUL server in accordance with the City User Password policy.*	Y	We are working towards changing the policy in CIS. The policy for accessing the PAUL server has already been completed. CIS and PAUL are secondary systems which require a user to first gain access to the City's network before they can be accessed. Access to the City's network is in compliance with the City User Password Policy.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		January 31, 2010 for CIS Setting
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
			Password setting for PAUL server completed in December 2009.

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
9	*Enable the password history setting on the PAUL server to prevent users from reusing the same password each time it is changed.*	Y	We have changed the password setting on the PAUL server. As previously mentioned, PAUL is a secondary system which requires a user to first gain access to the City's network before it can be accessed. Access to the City's network is in compliance with the City User Password Policy.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
			Completed December 2009

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
10	*Activate password settings for the Oracle user profiles in accordance with the City User Password policy.*	Y	We are in the process of completing this recommendation. Like CIS and PAUL, Oracle is a secondary system which requires a user to first gain access to the City's network before it can be accessed. Access to the City's network is in compliance with the City User Password Policy.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		2/28/10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION