Richmond City Council

The Voice of the People. Richmond, Virginia

OFFICE OF THE CITY AUDITOR

REPORT # 2011-03
AUDIT
of the

Richmond Department of Social Services Harmony System

August 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

Executive Summary……………………...……………….………………………...……………… i

Introduction, Audit Objectives and Background…………………...…...……..……………………… 1

Summary of Findings ……………………………...…………...……………...……………… 2

Management Responses………………………………………………………… Appendix A

City of Richmond
City Auditor

Executive Summary

Date: August 16, 2010

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

Subject: Harmony System Audit - Report 2011-03

The City Auditor's Office has completed an audit of the Harmony System in the Department of Social Services. The Harmony System is used by the Department of Social Services (DSS). The objective of this audit was to verify the existence of internal controls and evaluate the functionality of the system.

Professional Standards

Auditors followed Generally Accepted Government Auditing Standards and Control Objectives for Information and Related Technology guidelines issued by the Information Systems Audit and Control Association (ISACA).

What did the City Auditor's Office Find?

The general and application controls for the Harmony System need significant improvement. Auditors found deficiencies as follows:

Number of Deficiencies	Risk Involved
11	High
2	Medium
2	Low

Legend:

High Risk - Major deficiency resulting in a significant level of risk. Immediate management attention is required.
Medium Risk - 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.

The major risks that can have undesirable consequences if not addressed are:

- Data and information can be misused or manipulated without being detected in a timely manner.
- Potential for fraud exists.
- Unauthorized changes may not be detected and corrected in a timely manner.
- Due to lack of proper procedures, the potential for permanent loss of data exists.
- Unsecured data transmission may compromise sensitive information related to minors.
- Known issues in the current version of the system are not being addressed.
- The system, if failed, may not be successfully recovered due to lack of a business continuity plan.

Conclusion

Immediate management attention is required to address all the discrepancies labeled as high risk. The auditors have made 20 recommendations. The Department of Social Services has concurred with all of the recommendations.

The City Auditor's Office appreciates the Department of Social Services' cooperation during this audit. A written response to the report has been received and is included with this report.

Umesh Dalal, CPA, CIA, CIG
City Auditor

Summarized Report

Introduction

The City Auditor's Office has completed an audit of general controls (access to programs and data, program changes and backup and recovery) and application controls for the Department of Social Services (DSS) Harmony System. This audit covers the 12-month period ended June 30, 2009. The audit was conducted in accordance with Generally Accepted Government Auditing Standards 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 Harmony System and the recommendations presented.

Audit Objectives

- 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 the Harmony system and related IT controls and practices.

Background

Harmony is a mission critical case management system for DSS.

The Harmony Case Management System (Harmony) is designed specifically for the needs of Social Services Agencies. This software enables process automation, financial controls, and case management efficiency for different programs. The Harmony System includes functions such as intake and screening, scheduling and assessments, establishing and managing service plans, determining eligibility, invoice processing and vendor payments, and running case management reports.

The DIT support team and the DSS Help Desk are responsible for the day-to-day management of the System, including application administration, administering the infrastructure supporting the application, application security, managing changes, computer operations, and end-user support.

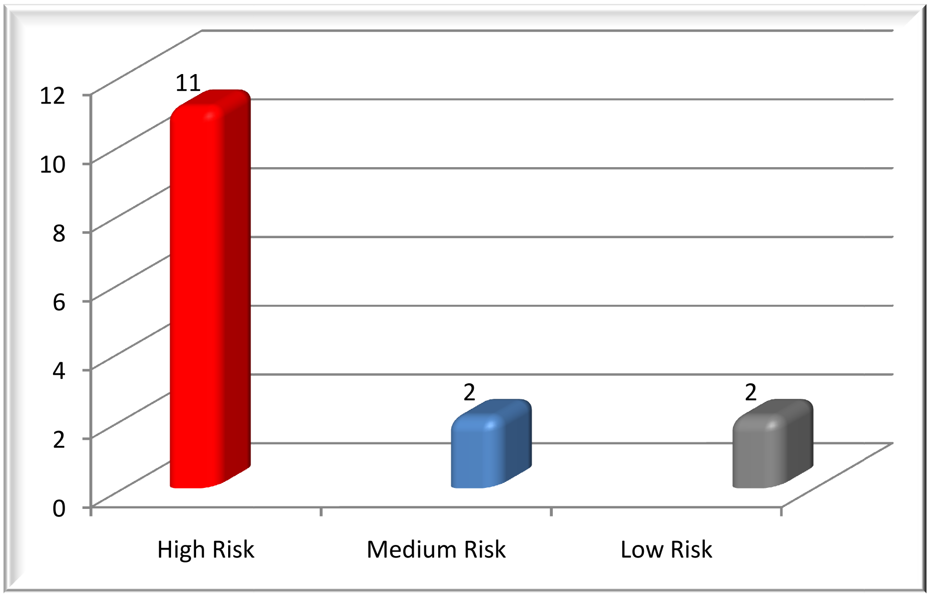
The table below depicts the summary of expenditures for different programs paid through Harmony during FY2009:

Program	Expenditures Spent For Each Program	% of Expenditures
At-Risk Youth and Family Services	$32,464,188	62.47%
Child Day Care	$8,375,155	16.12%
Adoption	$6,359,829	12.24%
Auxiliary Grant Programs	$3,293,981	6.34%
Adult Protective Services	$92,264	0.18%
Energy Assistance and General Relief	$621,678	1.20%
Adult And Aging Programs	$348,460	0.67%
Preservation of Family Unit Services	$204,254	0.39%
Companion Programs	$113,565	0.22%
Family Stabilization	$31,871	0.06%
VA Initiative for Employment not Welfare	$24,228	0.05%
Refugee Relief	$22,680	0.04%
Child Protective Services	$18,566	0.04%
Family Violence Services	$250	0.0005%
Total	$51,970,969.00	100.00%

Note: During FY2009, DSS overbilled the Virginia Department of Social Services approximately $3.4 million for Title IV-E payments. As a result, adjustments were made to CSA and Title IV-E programs to offset the overbilling. The summary of expenditures for each program shown in the table above was obtained after the adjustments were made to the Harmony System.

Summary of Findings

The following is the graphical presentation of the level of risk involved if the observed control weaknesses are not addressed:



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.

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 segregation of duties over the purchase order approval process: The Harmony System had 17 users with authority to perform all three levels of approvals (Case Worker, Supervisor, Finance), which allows employees to initiate and approve payments. Segregation of duties is a standard control procedure that prevents an individual from conducting all aspects of a transaction without proper checks and balances.	**Risk Level: High** Security risks over lack of segregation of duties for the purchase order approval process include: • Creating and processing invalid or fraudulent purchase order transactions. • Not adequately controlling purchase order transactions. • Intentionally modifying and processing existing purchase order data.	Restrict approval authority levels commensurate with the roles and responsibilities of the staff.
Lack of segregation of duties over vendor setup: The ability to add new vendors to the Harmony System is not restricted to the users from the Finance team.	**Risk Level: High** The risk of not restricting the vendor setup increases the likelihood of setting up fictitious vendors and making payments to them. There is a potential for fraudulent activity, which could result in financial loss to the City.	Limit the authority to add new vendors in Harmony to the Finance team only.
Inadequate password requirements: The Harmony security settings are not configured to require minimum length, expiration, and	**Risk Level: High** Without strong passwords, there is a greater potential for: • Gaining unauthorized access to the system by	Develop policies and procedures requiring the use of logical access authentication controls through the assignment of unique user IDs and strong passwords for all Harmony System users.

What did the auditors find?	What is the risk?	How to mitigate the risk?
lockout conditions of passwords. The Harmony System is supported by a SQL 2000 database. Password requirements cannot be configured on this version of SQL. Upgrading to the latest version of SQL will allow the above functionality. COBIT best practices require control over the IT process of ensuring systems security to safeguard information against unauthorized use, disclosure, modification, damage or loss.	guessing the passwords and masquerading as other users. • Gaining access to sensitive data and copying them for personal gain or use by another company. • Making unauthorized changes to the system software, modules, or applications.	Activate the password settings on the Harmony System and database.
Excessive administrator access accounts: There are nine (9) accounts with administrator access to the *Harmony System*. One of these accounts is a generic account, with no accountability of ownership. As recommended by COBIT, user access should be based on a "least privilege" and "need-to-know" basis. This ensures users have adequate access that is specifically and legitimately required for performing their assigned job duties.	**Risk Level: High** Without limiting administrative access to the appropriate individuals, there is a greater chance of unauthorized: • Changes to system software, data, modules, or applications. • Access to system resources. • Changes to system functionality by bypassing segregation of duties, edit checks, creating fictitious accounts and processing payments, etc. The above situation is undesirable and can be misused; therefore it should be addressed immediately.	Limit the administrator access to the Harmony and general supporting system to only a few individuals, preferably two or three users, who require such access to perform their roles and responsibilities.
Inappropriate administrator access accounts: There are 46 users with administrator access to the *Harmony server*. Only 8 of these users need such access to perform their job.	**Risk Level: High** These users can access the Harmony System as well as the underlying database, which creates a potential for abuse of the data and information.	Same as above.

What did the auditors find?	What is the risk?	How to mitigate the risk?
Lack of audit trail: Sensitive actions (e.g., granting system administration access, directly updating back end databases, etc.) performed by individuals with powerful application access such as System Administrators, Database Administrators, and Account Provisioning are not monitored in the Harmony System. Application audit trails of specific security related actions (e.g., security policy changes, login failures, etc.) in the system are not being logged and reviewed. It is prudent to review these changes periodically to verify that access privileges are not being abused.	**Risk Level: High** Without tracking data deletions and monitoring audit control logs, there is a risk that: • Unauthorized changes to system data are not tracked and the employee making data changes will not be determined. • Security violations and other activities like unsuccessful login attempts are not being logged, tracked and addressed • Users cannot be held accountable for their actions.	Assess the feasibility of turning on the audit trail feature to capture significant events, including: All access attempts (successful and failed) Activities performed by users with special privileges. Changes to significant files or security configuration settings.
Lack of approved backup policy: The backup policy is a draft and has not been finalized. Harmony System backups are performed every day, except on Fridays and Mondays. Also, there is no periodic backup testing to verify the integrity of the backup tapes and the ability to restore systems and data from tapes. 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** Without proper system backup, DSS runs the risk of permanently losing the data and severe disruptions to the DSS operations if the Harmony System goes down.	Finalize the DIT 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. Backup the Harmony servers on a daily basis. Create a formal process of recording all successful and unsuccessful backups to document the validity and reliability of the backup process. Create a formal process for performing a periodic tape restore testing and document the results showing both successful and unsuccessful backups from tape.

What did the auditors find?	What is the risk?	How to mitigate the risk?
Sensitive information transmitted over unsecured Internet connection: The Comprehensive Services Act (CSA) reporting data which includes personal identification information (name, social security number, etc.) is transmitted to Virginia Department of Social Services (VDSS) via email over the Internet and is not encrypted as required by the VDSS policy. The VDSS Information Security Standard requires sensitive information to be encrypted when it is transmitted over the Internet. The State has a website to accept encrypted transmission that is being used by several jurisdictions. The City of Richmond is not using this website.	**Risk Level: High** Without encryption, there is an increased risk of: ➢ Confidential information being intercepted while data is sent over public accessible network lines. This increases the risk of a data breach and identity theft that could result in lawsuits and penalties to the City. ➢ Confidential information being compromised when changes are made by an attacker as data is being transmitted. ➢ Changes made to system files by an attacker creating a backdoor to access the system.	Work with VDSS and DIT to enforce strong encryption procedures prior to transmitting the data set information to VDSS.
Outdated version of Harmony has known issues: DSS is using an outdated version of the Harmony software. Because of this, DSS is not taking advantage of the enhancements that would address some of the known issues and new features that would significantly improve their business process. Addressing this issue will improve efficiency and effectiveness of the services provided and related controls in DSS procedures.	**Risk Level: High** The risks of using an outdated software application include: • DSS has to perform manual work around the existing bugs. The manual work introduces the potential of human errors, and increases the risk that application functionality will not execute in accordance with Management's expectations. • There are known defects in the current version which the newer version addresses. • Lack of vendor support in the future.	Work with DIT and Finance to upgrade to the most recent version of the Harmony software. After upgrading, retire the client server Harmony application and remove the software from all user computers. *The vendor proposal received in April 2008 quoted the cost to perform the upgrade of less than $10,000.*

What did the auditors find?	What is the risk?	How to mitigate the risk?
Major security gaps in Harmony: The Harmony client server application has major security gaps that could compromise the integrity of data.	**Risk Level: High** The security gaps increase the risk that end users may use the system in a manner that: • Compromises the security posture of the system and data. • Unauthorized activities have gone and/or will go undetected by management.	Same as above.
Business Continuity Plan needs to be finalized: The DSS COOP is a draft and needs to be finalized, approved and tested. COBIT recommends that IT continuity plans be designed to reduce the impact of a major disruption on key business functions and processes.	**Risk Level: High** The lack of a finalized COOP increases the risk that key business processes would not be correctly and/or efficiently reinstituted in the event of a disaster that renders the system temporarily unusable. Failure to adequately educate individuals tasked with key recovery responsibilities increases the risk that an actual recovery effort is incorrectly executed. This in turn could result in a delayed recovery or a recovery that comprises the system's ability to process data and/or business processes.	Work with Emergency Operations to finalize the COOP. Conduct testing and document the results of testing to examine the effectiveness of the COOP. Provide all staff with regular COOP 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.
Accountability of vendor refund checks needs improvement: The vendor refund functionality is not currently being used by DSS to process refunds from vendors in the Harmony System.	**Risk Level: Medium** Not properly recording refund checks could lead to overbilling VDSS. In a recent audit, this risk was found to have materialized.	Train users on how to process vendor refunds on the Harmony System and start using this function to process refunds. Also, work with the Harmony vendor and DIT to automatically transmit the refund information to the Advantage Financial System.
User access needs to be monitored: Periodic review of the defined	**Risk Level: Medium** Failure to perform periodic reviews increases the risk that	Create and implement a policy to periodically review and recertify user access to the Harmony System and the database.

What did the auditors find?	What is the risk?	How to mitigate the risk?
user groups and user access with the Harmony System is not performed. This is a prudent practice to assure security of data and information.	individuals have unauthorized access to the system.	Document the review results and their resolution.
Duplication of efforts exists: When setting up new cases during the intake process for foster care, some of the children's information is keyed into both the Harmony and VDSS systems.	**Risk Level:** Low Duplicate data entry leads to decreased employee productivity.	Work with VDSS to determine whether case information captured in the VDSS System can be automatically transferred to the Harmony System.
Completion of Harmony access request forms needs to be consistent: Supervisors do not consistently complete Harmony Access Request forms or document approvals (security officer and supervisor) prior to establishing access on the Harmony System.	**Risk Level:** Low Users can have unauthorized access to the system that is inconsistent with their job responsibilities.	Establish and enforce a formal written security policy outlining the approval requirements for granting, modifying and removing access to the Harmony system. This policy should promote the principle of "least privilege" whereby access to information and system resources is assigned to individuals based upon the minimum level of access necessary to perform their job responsibilities.

MANAGEMENT RESPONSE FORM
DEPARTMENT OF SOCIAL SERVICES

APPENDIX A

HARMONY SYSTEM AUDIT - REPORT #2011-03

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
1	*Restrict approval authority levels commensurate with the roles and responsibilities of the staff.*	Y	As of 04/10/10 only Finance staff has all 3 levels of approval. There are a total of 7 users, all of which are located in Finance. Additionally, two separate log-in's have been created for keying of invoices that do not have the full approval access and a policy has been put in place in Finance to ensure all POs, Invoices, and Payables have at least 2 levels of approval with supporting documentation. Additional testing is underway to see if a level can be removed from finance to drop that number to 0. Estimated completion of this testing is 09/01/10.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		1-Sep-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
2	*Limit the authority to add new vendors in Harmony to the Finance team only.*	Y	As of 4/1/10 only 2 groups (Finance-1 and Finance) have access to add vendors, totaling 15 users. This number will be further reduced to 3 primary workers in Fianace responsible for vendor entry into Harmony through user group segregation. This task will be completed by 09/01/10.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		1-Sep-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
3	*Limit the administrator access to the Harmony and general supporting system to only a few individuals, preferably two or three users, who require such access to perform their roles and responsibilities.*	Y	The number of users with system administrator level access has dropped to 5. This staff only includes the Harmony system administrator and RDSS technical support team staff. In addition to this reduction, all system administrators have had the three levels of approval removed to ensure no improper payment processing. This number will be further reduced to 2 users with full system administrator rights and 3 with special limited rights that allows only password updates. This will be completed by 08/13/10. DIT has removed their Systems Developer as an administrator on the DSSHarmony03 database server. This leaves only the two DBA accounts, Domain Admins, HarmonyVPN (disabled), and Web Server Admins groups with the ability to perform administrator level functions on the server.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		13-Aug-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
4	*Develop policies and procedures requiring the use of logical access authentication controls through the assignment of unique user IDs and strong passwords for all Harmony System users.*	Y	Completed on 07/12/10. DIT approved password requirements were put into effect. These requirements were reviewed by Audit and received approval based upon DIT standards. RDSS worked with DIT to utilize the change control procedure for this effort (see CCN 8264, closed on 7/14/2010). RDSS will work with DIT in the future to adopt this as a standard procedure.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Business Analysis Manager		12-Jul-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
5	*Activate the password settings on the Harmony System and database.*	Y	The recommended password settings were tested and implemented in the production database on 07/12/10. These requirements were reviewed by both DIT and the Audit Office prior to implementation. DSS received approval of the settings based upon established DIT password standards. RDSS worked with DIT to utilize the change control procedure for this effort (see CCN 8264, closed on 7/14/2010). RDSS will work with DIT in the future to adopt this as a standard procedure.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Business Analysis Manager		12-Jul-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
6	*Assess the feasibility of turning on the audit trail feature to capture significant events, including the following:* *• All access attempts (successful and failed.)* *• Activities performed by users with special privileges.* *• Changes to significant files or security configuration settings.*	Y	Upgrading Harmony to its most current version will aide in tracking further updates/configuration settings in the system. RDSS will work with DIT and Audit to ensure the tracking requirements are clearly defined so the requirements can be met. DIT will also work with RDSS to identify the information that can be captured by the PacketSentry product to meet the needs of this requirement.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Systems Operations Administrator		9/30/2010
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
7	*Establish and enforce a formal written security policy outlining the approval requirements for granting, modifying and removing access to the Harmony system. This policy should promote the principle of "least privilege" whereby access to information and system resources is assigned to individuals based upon the minimum level of access necessary to perform their job responsibilities.*	Y	RDSS is establishing formal documentation outlining the system access request process being followed for obtain access to the Harmony system. The policy is being based on the practice of granting "least privilege" level of access to users. A formal policy will be presented to Deputy Director of Finance and Administration by 09/30/10 for review and approval. Harmony access is currently part of the System Access Privilege Request (SAPR) process, but that form does not include all the details necessary to properly configure a user's access in Harmony. DIT and RDSS will add this to the RDSS Technology Roadmap as a new project to expand the SAPR form to include the missing details.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Systems Operations Administrator		30-Sep-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
8	*Create and implement a policy to periodically review and recertify user access to the Harmony System and the database.*	Y	The policy is currently in draft form and being reviewed. RDSS has implemented quarterly reviews to review and rectify user acess.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Systems Operations Administrator		30-Sep-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
9	*Document the review results and their resolution.*	Y	The Harmony administrator and the DSS technical support team have implemented a review process to routinely review access for all users to Harmony applications. This review cycle ensures that all accounts are reviewed quarterly. The results are being documented and a file maintained of the results for audit review.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Systems Operations Administrator		30-Sep-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
10	*Finalize the DIT 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	DIT takes a backup each business day of the Harmony production database. Creation of the DIT backup policy is in the final stages and should be completed no later than 09/30/2010. DIT will work with RDSS to schedule restore testing.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Systems Operations Administrator		30-Sep-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
11	*Backup the Harmony servers on a daily basis.*	Y	This recommendation has already been implemented. Backups of the Harmony production database are conducted each business day as follows: Incremental - Monday - Friday evening after the business day. Full - Monday morning prior to start of the business day.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Systems Operations Administrator		13-Sep-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
12	*Create a formal process of recording all successful and unsuccessful backups to document the validity and reliability of the backup process.*	Y	Creation of the DIT backup policy is in the final stages and should be completed no later than 09/30/2010.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Systems Operations Administrator		30-Sep-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
13	*Create a formal process for performing a periodic tape restore testing and document the results showing both successful and unsuccessful backups from tape.*	Y	DSS is working with DIT to define the restoration procedure ensuring periodic restoration testing is conducted and the test results are documented.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Systems Operations Administrator		30-Sep-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
14	*Work with VDSS and DIT to enforce strong encryption procedures prior to transmitting the data set information to VDSS.*	Y	RDSS is working with the OCS (Office of Comprehensive Services) contractor to test uploading of the data via the OCS website to ensure the data is submitted via a SSL connection. Retrieval of error reports using the same method is also being tested to ensure the entire process meets the data encryption requirements. This process is currently in use by other localities that submit a quarterly CSA dataset to OCS. Initial testing was successful on 08/10/2010. Final testing will occur on 08/13/2010. The process is being documented as testing takes place and will be finalized upon successful completing of testing.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Systems Operations Administrator		13-Aug-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
15	*Work with DIT and finance to upgrade to the most recent version of the Harmony software. After upgrading, retire the client server Harmony application and remove the software from all user computers.*	Y	Upgrading the system is the established recommendation. This recommendation requires upper management support and financial approval to proceed. A meeting has been scheduled with Harmony to discuss future upgrades and interfaces which will be held on 9/8/2010. RDSS is performing a business process analysis with assistance from DIT. This effort will aid in the decision to upgrade or replace the software.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		1-Nov-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
16	*Train users on how to process vendor refunds on the Harmony System and start using this function to process refunds. Also, work with the Harmony vendor and DIT to automatically transmit the refund information to the Advantage Financial System.*	Y	RDSS is currently investigating a way for the Harmony system to interact with Advantage to process refunds without using the current process of manual cash entry. In lieu of a formal automated process, Finance will record all vendor refunds in same process of returned checks for proper reporting to Laser and CSA Pool. A policy draft for this is currently under review. RDSS is performing a business process analysis with assistance from DIT. This effort will aid in the decision to upgrade or replace the software and this process will be addressed in that effort.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		1-Nov-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
17	*Work with VDSS to determine whether case information captured in the VDSS System can be automatically transferred to the Harmony System.*	Y	The long term goal is to create an interface with state programs for Harmony upload of required data. This is a secondary step to upgrading harmony system to the most current version. DIT will work with RDSS to approach VDSS about options for sending and receiving data on a daily basis.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Business Analysis Manager		31-Dec-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
18	*Work with Emergency Operations to finalize the COOP.*	Y	The agency's COOP plan was revised and submitted to City's Office of Emergency Management for recommendations and approval. Discussions with DIT, VDSS, and VITA/NG are ongoing to clarify how the agency's COOP plan needs to be tied in with those agencies plans. RDSS is heavily reliant on those agencies that provide RDSS with network services, application hosting and computer hardware which are crucial to the agency being able to conduct essential functions.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Administrative Services Manager		31-Dec-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
19	*Conduct testing and document the results of testing to examine the effectiveness of the COOP.*	Y	RDSS is working on developing a COOP testing strategy. RDSS will be contacting the Office of Emergency Management for their assistance and will arrange tabletop exercises. Results will be documented and reviewed to identify any weaknesses in the plan.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Administrative Services Manager		31-Dec-10
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
20	*Provide all staff with regular COOP 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	RDSS is contacting the Office of Emergency Management for training guidance and will utilize in-house training staff to develop routine COOP training for all agency staff. Training sessions will be targeted to begin during the 3rd quarter of FY11.
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Administrative Services Manager		31-Jan-11
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**