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

REPORT # 2011-05
AUDIT
Of the

Richmond City Fire Records Management System

January 2011

OFFICIAL GOVERNMENT REPORT

Richmond City Council
OFFICE OF THE CITY AUDITOR
900 East Broad Street, 8th Floor
Richmond, Virginia 23219

804.646.5616 (tel); 804 646.2230 (fax)

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

TABLE OF CONTENTS

City of Richmond
City Auditor

Executive Summary

January 31, 2011

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

Subject: Fire System Audit - Report 2011-05

The City Auditor's Office has completed an audit of the Fire Records Management System (FRMS) in the Department of Fire and Emergency Services. The objectives of this audit were to verify the design and effectiveness of internal controls, to review the reasonableness of resources committed to FRMS implementation, and to 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 internal controls for the FRMS need significant improvement. Auditors found deficiencies as follows:

Number of Deficiencies	Risk Involved
8	High
3	Medium
1	Low

For additional details regarding the deficiencies, see the summarized report.

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

- Poor project management contributed to the delay of the project and the projected visions and capabilities of the FRMS have not been fully met.
- There is no performance monitoring of the FRMS vendor and the service has become poor.
- Adequate testing has not been performed and the implemented modules have bugs that should have been addressed prior to implementation.
- The system, if failed, may not be successfully recovered due to lack of business continuity plan testing.
- Inadequate password requirements could lead to unauthorized use, disclosure, modification, damage or loss of FRMS data.
- Terminated users have access to the network and the FRMS application and this could lead to potential abuse of the data and information
- The water based fire suppression system could damage IT equipment and systems if exposed to water.
- There are a lack of policies, procedures and guidelines for managing FRMS security.

Conclusion

Immediate management attention is required to address all the discrepancies labeled as high and medium risk. If the discrepancies are not addressed, they could lead to:

- Inefficiencies in operations that would impact the essential functions such as: management reporting, duplicate data entry and data analysis.
- Inability to report fire incidents and emergency medical services to the regulatory agencies.

The auditors have made 28 recommendations. The Department of Fire and Emergency Services has concurred with 24 of the recommendations.

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

Umesh Dalal, CPA, CIA, CIG
City Auditor

#	*COMPREHENSIVE LIST OF RECOMMENDATIONS*	*PAGE*
1	**Hold the Fire Department and DIT management accountable to complete the implementation of the remaining FRMS modules and interfaces by the deadline.**	4
2	**Ensure that the program is properly staffed in order to complete the project within a reasonable time period.**	4
3	**Develop performance measures to demonstrate how the efficient and effective use of the FRMS helps the Fire Department achieve its business goals.**	4
4	**Perform vendor performance evaluation pursuant to the established SLA and the City procurement policy.**	4
5	**Work with the Office of Emergency Management to finalize the DIT COOP.**	5
6	**Conduct testing and document the results of testing to examine the effectiveness of the COOP.**	5
7	**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.**	5
8	**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.**	5
9	**Backup the FRMS data and servers on a daily basis.**	5
10	**Create a formal process of recording all successful and unsuccessful backups to document the validity and reliability of the backup process.**	6
11	**Create a formal process for performing a periodic tape restore testing and document the results showing both successful and unsuccessful backups from tape.**	6
12	**Once the termination policy is established, enforce the procedures related to removing separated user access within the network and FRMS in a timely manner.**	6
13	**Work with the vendor to activate the password settings on FRMS.**	6
14	**Upgrade the SQL database to SQL2008 as the current version (SQL 2000) does not support password functionality.**	6
15	**Perform testing to determine whether the Supervisor ID account can be disabled with no adverse effect to system maintenance and function.**	7
16	**Remove GIS Analyst from the Supervisor group and add him to a group that is limited to accessing information relevant to his job responsibilities.**	7
17	**DIT_NT4_Admins group has administrative access to the FRMS database server. Restrict DIT_NT4_Admins group members to the Network Engineers team.**	7
18	**Upgrade the existing fire suppression system to have both gaseous and water based (pressurized dry pipes) fire suppression systems.**	8

19 Continue phased replacement and upgrades to the major heating, air conditioning, ventilation, administrative space and electrical system in the Data Center as per the Capital Improvement Project. 8

20 Establish a formal written security policy outlining the approval requirements for granting, modifying and removing access to FRMS. 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. 8

21 Develop policies and procedures requiring the use of logical access authentication controls through the assignment of unique user IDs and strong passwords for all FRMS application users. 9

22 Develop policies and procedures for managing changes including minor application changes, major application changes and software releases. This should include procedures for testing and receiving proper authorization and are supported by a change request document. 9

23 Implement change management procedures to ensure that all application changes and upgrades are approved, tested and documented prior to implementation. 10

24 Periodically review the user access to FRMS and the database. 10

25 Document the review results and their resolution. 10

26 Document the data interfaces with the outbound (i.e. submitting) and inbound (i.e. receiving) systems. The documentation should include at a minimum, the following items: 10

• Data Elements contained within the interface;
• Frequency of the interface;
• Volume of transactions flowing through the interface;
• Individual responsible for the operation of the data interface;
• High-level business purpose for the interface;
• High-level technical design description or diagram for the steps in the interface process, and;
• Integrity of the data.

27 Work with the FRMS vendor to determine if NFPA fire codes can be uploaded instead of keying them into FRMS. 11

28 Create an automated interface with the Proval system to import properties information. 11

City of Richmond Audit Report
Department of Fire and Emergency Services
Fire Records Management System Audit 2011-05
Fiscal Year 2010

Introduction

The City Auditor's Office has completed an audit of general controls for the Fire and Emergency Services Department's Fire Record Management System. This audit covers the 12-month period ended June 30, 2010. The audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and Control Objectives for Information and related Technology (COBIT) guidelines issued by the Information Systems Audit and Control Association (ISACA). Those standards provide a reasonable basis for the conclusions regarding the internal control structure over the Fire Records Management System (FRMS) and the recommendations presented.

Audit Objectives

- Determine whether adequate IT general controls for access to programs and data, program development, change management, data transmission and backup and recovery have been established by management;
- Review the reasonableness of resources committed to implementing FRMS, support and training; and
- Evaluate the compatibility with current and future systems.

Background

FRMS is the system of record for fire incidents, investigations, inspections and medical services.
Prior to FRMS, the Fire and Emergency Services Department used FirePro as their records management system. FirePro became obsolete and did not meet the new Federal and State requirements for collecting and reporting emergency response data. Therefore, it was replaced by FRMS, which provides a significant improvement in the Fire Department's ability to conduct broad and specific data analysis, performance measuring and reporting.

FRMS is specifically tailored for Fire and Emergency Management Services (Fire) agencies. FRMS is a complete "off-the-shelf" application that manages daily operations, including standard forms and reports for data analysis. The FRMS application has modules (i.e. Incidents, Inspections, Permits, Training, and Properties) for managing daily operations. Data is shared across modules to eliminate duplicate data entry and reducing the chance of error.

FRMS is administered by two (2) users who are responsible for the day-to-day management of the system, including application administration, application security, computer operations, and end-user support. The Department of Information Technology team is responsible for maintaining the support systems (fire database and server).

The Fire and Emergency Services Department performs several key functions to educate and protect the public. The Department is divided into four divisions: Prevention, Operations, Support Services, and Emergency Services.

Fire Prevention: This Division is dedicated to the protection of life and property. It is responsible for public education (a pro-active effort to lessen the number of incidents), code enforcement (responsible for the inspection of commercial facilities, issuing violation notices, issuing summons, issuing permits, and investigating complaints), and fire investigations (fire fatality, multi-alarm fires, bomb threats, large dollar loss, and suspicious fires)

Fire Operations: This Division is responsible for protecting the citizens against injury and loss of life/property caused by fire.

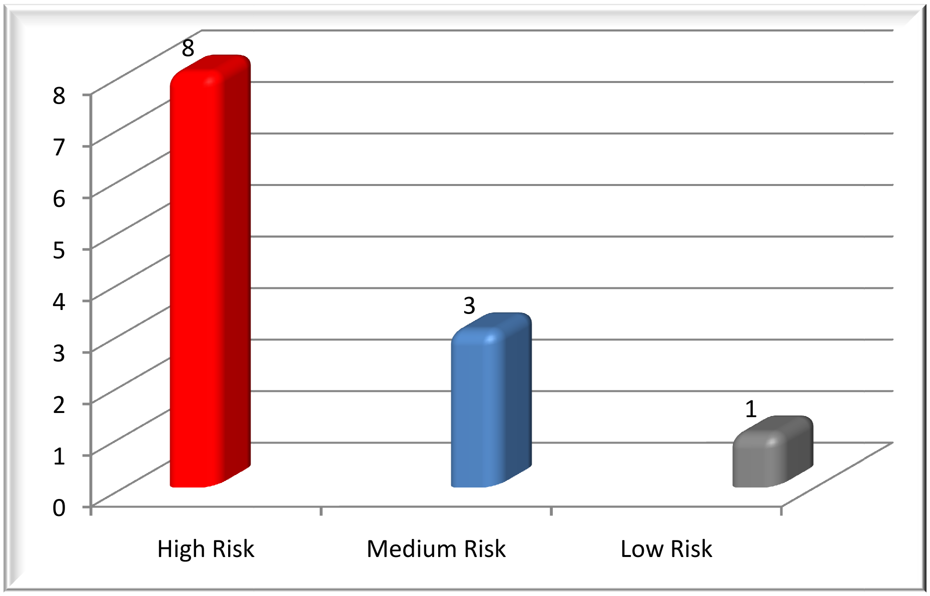
Support Services: This Division is responsible for logistical support and purchasing functions.

Emergency Services: This Division is responsible for providing emergency medical services to injured personnel.

FRMS is a critical system to the Fire and Emergency Services Department since it is used for the daily operations of the Fire Department, and holds the department data used for management reporting and interfaces with state and federal reporting systems.

Summary of Findings

The following is the graphical presentation of the level of risk involved for the identified control weaknesses:



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.

Overall Conclusion

Immediate management attention is required to address all the discrepancies labeled as high and medium risk. If the discrepancies are not addressed, they could lead to:

- Inefficiencies in operations that would impact the essential functions such as: management reporting, duplicate data entry and data analysis.
- Inability to report fire incidents and emergency medical services to the regulatory agencies.

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?
Poor project management and inadequate management support: The project implementation was delayed from the beginning of the project due to lack of dedicated full time resources from DIT and the Fire Department. In addition to the staffing limitations, both the vendor and DIT changed the project managers during the project implementation phase. Inadequate time was provided in the project plan to ensure sufficient time to complete tasks properly and to test, re-test and sign-off on all interface, data validations and integration points.	**Risk Level: High** The lack of dedicated and conversant resources delayed the completion of project activities and could ultimately impact the project budget and also run the risk of installing outdated versions of the system. Poor project management impacted the project deliverables and completion of the project. Inadequate time and resources allocated to test the system led to problems (both significant and minor) that were not uncovered during testing leading to production problems.	1. Hold the Fire Department and DIT management accountable to complete the implementation of the remaining FRMS modules and interfaces by the deadline. 2. Ensure that the program is properly staffed in order to complete the project within a reasonable time period.
Major deficiencies in implementation of the system: The business requirements were not sufficiently detailed and thus inadequate. Consequently no traceability matrix could be created which would allow the Fire Department to validate that the system met the functional requirements. DIT was not able to provide any evidence that the following project tasks had been completed for FRMS at its	**Risk Level: High** The absence of performance measures increases the risk that the investment is not meeting the key business objectives of the Department and that resources committed to the project may thus be wasted. The absence of formal vendor performance evaluation increases the risk that sub-par	3. Develop performance measures to demonstrate how the efficient and effective use of the FRMS helps the Fire Department achieve its business goals. 4. Perform vendor performance evaluation pursuant to the established SLA and the City procurement policy.

What did the auditors find?	What is the risk?	How to mitigate the risk?
outset: - Risk assessment and mitigation. - Performance measurements used to monitor the effectiveness of FRMS and the vendor. - Cost-benefit, cost savings, return on investment (ROI) analyses.	performance is not reported and evaluated in order for the City to take appropriate action to improve performance or cancel the contract. Consequently, excessive resources may continue to be spent without achieving the purpose for which the contract was originally intended.	
Business Continuity Plan needs to be tested: The Fire Department COOP was not finalized until August 2010. Therefore testing had not been performed during the audit scope. The DIT 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 of 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 resumed 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 would be improperly executed. This in turn could result in a delayed recovery or a recovery that compromises the system's ability to process data and/or business processes.	5. Work with the Office of Emergency Management to finalize the DIT COOP. 6. Conduct testing and document the results of testing to examine the effectiveness of the COOP. 7. 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.
Lack of approved backup policy: FRMS tape backups are not performed on Tuesdays and Thursdays. 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.	**Risk Level: High** Without proper system backup, the Fire Department runs the risk of permanently losing the data if the system suffers interruptions.	8. 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. 9. Backup the FRMS data

What did the auditors find?	What is the risk?	How to mitigate the risk?
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.		and servers on a daily basis. 10. Create a formal process of recording all successful and unsuccessful backups to document the validity and reliability of the backup process. 11. Create a formal process for performing a **periodic** tape restore testing and document the results showing both successful and unsuccessful backups from tape.
Terminated users having access to the systems: There are 29 users who are no longer employed at the City but still have active FRMS accounts. Out of these 29 users, there are five (5) users who also had active network accounts to log in to the City's network.	**Risk Level: High** These users can access FRMS, which creates a potential for abuse of the data and information.	12. Once the termination policy is established, enforce the procedures related to removing separated user access within the network and FRMS in a timely manner.
Inadequate password requirements: FRMS has limited password functionality and cannot enforce strong passwords such as requiring: • the passwords to be of a certain length • the password history not to allow recently used passwords • password complexity Password expiration is not set on FRMS to force users to change passwords	**Risk Level: High** Without strong passwords, there is a greater potential for: a. Gaining unauthorized access to the system by guessing the passwords and masquerading as other users. b. Gaining access to sensitive data and copying them for personal gain or use by another company. c. Making unauthorized	13. Work with the vendor to activate the password settings on FRMS. 14. Upgrade the SQL database to SQL2008 as the current version (SQL 2000) does not support password functionality.

What did the auditors find?	What is the risk?	How to mitigate the risk?
periodically. FRMS is supported by a SQL 2000 database. Password requirements cannot be configured on this version of SQL. Upgrading to the latest version of SQL2008 will allow the above functionality. The cost of the standard SQL2008 software will be less than $1,000 dollars as the City has an enterprise agreement with the vendor. COBIT best practices require control over the IT process of ensuring systems security to safeguard information against unauthorized use, disclosure, modification, damage or loss.	changes to the system software, modules, or applications.	
Excessive administrator access accounts: Administrator privileges provide access to all tables in FRMS. Administrator privileges allow users to add or delete other users, assign users to groups, and define rights for security groups. There are four (4) accounts belonging to the Administrator group that provide them with administrator access privileges to FRMS. One of these accounts belongs to the GIS Analyst. The GIS Analyst has access to all database tables due to administrative privileges. His administrative access should be removed and added to a group that is limited to accessing information relevant to his job responsibilities. Also, there is a generic account (Supervisor ID) with no accountability of ownership.	**Risk Level: High** Without limiting administrative access to the appropriate individuals, there is a greater chance of unauthorized: a. Changes to system software, data, modules, or applications. b. Access to system resources. c. 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.	15. Perform testing to determine whether the Supervisor ID account can be disabled with no adverse effect to system maintenance and function. 16. Remove GIS Analyst from the Supervisor group and add him to a group that is limited to accessing information relevant to his job responsibilities. 17. DIT_NT4_Admins group has administrative access to the FRMS database server. Restrict DIT_NT4_Admins group members to the Network Engineers team.

What did the auditors find?	What is the risk?	How to mitigate the risk?
DIT_NT4_Admins group has administrative access to the FRMS database server. There are members outside of the DIT Network Engineers team that have access to this group. 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.		
Upgrade Fire Suppression: The Data center has a water based fire suppression system. The IT equipment and systems can short or become damaged if exposed to water.	**Risk Level: High** The IT equipment and systems will be damaged if exposed to water. The common practice for fire suppression in the Data Center is to have both gaseous and water based fire suppression systems. The gaseous system is invoked to suppress a fire and then the water based fire sprinkler system is deployed if the fire is still raging.	18. Upgrade the existing fire suppression system to have both gaseous and water based (pressurized dry pipes) fire suppression systems. 19. Continue phased replacement and upgrades to the major heating, air conditioning, ventilation, administrative space and electrical system in the Data Center as per the Capital Improvement Project.
Lack of security policies and procedures: Management has not documented and communicated security policies and procedures that provide the overall	**Risk Level: Medium** When user account management and authentication policies for granting,	20. Establish a formal written security policy outlining the approval requirements for granting, modifying and removing access to FRMS. This policy

What did the auditors find?	What is the risk?	How to mitigate the risk?
framework for managing FRMS security and guidelines for enforcing information security controls. The security policies and procedures should include coverage of the following areas: 1. The process and associated roles and responsibilities for requesting and approving user access to FRMS and general systems supporting FRMS. 2. The process and associated roles and responsibilities for terminating access to the FRMS and general support systems. 3. The process and associated roles and responsibilities to review user access rights to the FRMS and general support systems. The review should include: a. A log of any exceptions noted; b. The final disposition of exceptions; and c. The final approval of user access rights per system. 4. A security policy requiring the use of logical access authentication controls through the assignment of unique user IDs and strong passwords for all users of FRMS. This policy should recognize that different systems have different access control capabilities and that the strongest combined (or layered) series of access controls should be enforced. 5. The process and associated roles for requesting, tracking, approving and testing minor application fixes, major application fixes and product releases.	modifying, removing or authenticating access to the FRMS system are not set forth and therefore not communicated to all stake holders, there is a potential for users to have inappropriate access to information, applications, and infrastructure that are not required for their job responsibilities. Lack of policies and procedures for managing FRMS changes could lead to unauthorized changes or inadequately tested changes to be deployed to production.	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. 21. Develop policies and procedures requiring the use of logical access authentication controls through the assignment of unique user IDs and strong passwords for all FRMS application users. 22. Develop policies and procedures for managing changes including minor application changes, major application changes and software releases. This should include procedures for testing and receiving proper authorization and are supported by a change request document.

What did the auditors find?	What is the risk?	How to mitigate the risk?
Change request documentation: There is no evidence of documentation supporting the management approval and testing for FRMS changes.	**Risk Level: Medium** Lack of or weak change management controls may lead to: a. Inaccurate or incomplete business data; b. Failed system; and c. Data and systems exposed to inside and outside vulnerabilities.	23. Implement change management procedures to ensure that all application changes and upgrades are approved, tested and documented prior to implementation.
User access needs to be monitored: Periodic review of the defined user groups and user access to FRMS is not performed. This is a prudent practice to assure security of data and information.	**Risk Level: Medium** Failure to perform periodic reviews increases the risk that individuals have unauthorized access to the system.	24. Periodically review the user access to FRMS and the database. 25. Document the review results and their resolution.
Lack of automated interfaces: There is no automated FRMS interface with Proval to import property information. National Fire Protection Association (NFPA) fire code changes have to be manually keyed into FRMS. There is no built in functionality to upload the fire codes.	**Risk Level: Low** The lack of automated interface for data transfer: 1. Increases the processing time and man hours. 2. Could lead to manual keying errors. 3. Makes it difficult to test the completeness and accuracy of data.	26. Document the data interfaces with the outbound (i.e. submitting) and inbound (i.e. receiving) systems. The documentation should include at a minimum, the following items: • Data Elements contained within the interface; • Frequency of the interface; • Volume of transactions flowing through the interface; • Individual responsible for the operation of the

What did the auditors find?	What is the risk?	How to mitigate the risk?
		data interface; • High-level business purpose for the interface; • High-level technical design description or diagram for the steps in the interface process, and; • Integrity of the data. 27. Work with the FRMS vendor to determine if NFPA fire codes can be uploaded instead of keying them into FRMS. 28. Create an automated interface with the Proval system to import properties information.

ATTACHMENT A: MANAGEMENT RESPONSE FORM

FIRE RECORDS MANAGEMENT SYSTEM AUDIT REPORT #2011-05

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
1	***Hold the Fire Department and DIT management accountable to complete the implementation of the remaining FRMS modules and interfaces by the deadline.***	**Yes**	*Weekly meetings with Chief Thomas and APA Smith to review and chart progress with proposed timeline. Follow up meetings with vendor, DIT and other ad hoc representatives when and where appropriate, but a minimum of monthly.*
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	SBC and DIT Director		**12/31/2011**
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
	The Department has been working with the vendor (FDM) to identify which modules require additional work. Because of an OEMS mandate that required the submission of NEMSIS compliant patient medical records, much of the project scope was put on hold to achieve this regulatory requirement. All personnel from both the department and vendor were re-allocated to this function which delayed the implementation of remaining modules/interfaces and certain aspects of re-work to various in-place modules.		
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
2	***Ensure that the program is properly staffed in order to complete the project within a reasonable time period.***	**Yes***	*(1) Work with finance and City Administration to create two (2) additional dedicated, IT conversant civilian FTE's to support the departments FRMS needs, as a short term back up, attempt to arrange a temporary assignment of DIT personnel specific to this initiative while recruiting a permanent solution. (2) Schedule a meeting with the DIT director, the purpose of the meeting will be to ensure that both entities have an opportunity to review the audit findings with respect to this line item and each entity takes appropriate interal action to address the staffing component with adequate and timely resources.*
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	SBC		**(1) FY 12-13 and (2) 2/28/11**
	IF IN PROGRESS, EXPLAIN ANY DELAYS		**IF IMPLEMENTED, DETAILS OF IMPLEMENTATION**
	The department has one (1) FTE allocated to department wide IT support (help desk functions). This position is supplemented by one (1) FTE that has been transferred (under a long term arrangement) from field staffing. Between the two of them, they have been solely responsible for every IT initiative within the department. Recognizing the limitations this model presented, the department recently re-defined the the role of one of the APAs (C. Smith -- who just returned from a "x" month military deployment) to assist with project implementation.		
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
3	***Develop performance measures to demonstrate how the efficient and effective use of the FRMS helps the Fire Department achieve its business goals.***	**Yes**	*(1) A review of the original contracting documents and vendor capabilities (with specific emphasis) on the various modules will be conducted. This will compare department expectations, vendors stated capabilities and the actual output. From this review, the respective performance measures will be defined. (2) Separately, a review of industry literature, best practices and accreditation standards will continue to develop performance measures for the department that can be tracked/trended using FRMS within the implemented modules. This will help benchmark future design issues within FRMS as module enhancements are developed.*
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	SBC		**12/31/2011**

	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
	Several modules require additional 'clean-up' and functionality testing to ensure they are customized sufficiently to allow this desired function. The lack of effective implementation and insufficient FTE allocation has delayed the departments full realization of using FRMS. (i.e., asset management module for tracking expenditure and replacement; Roster for time management and payroll; Incidents for customization of NFIRS reporting and subsequent ICMA benchmarking studies).		
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
4	***Perform vendor performance evaluation pursuant to the established SLA and the City procurement policy.***	Yes	*Ensure the periodic progress with the project timeline (as developed) is documented, using the language within the existent SLA framework. Additionally ensure all maintenance requests are submitted (and documented) within the framework.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	SBC		**2/1/2011**
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
5	***Work with the Office of Emergency Management to finalize the DIT COOP.***	Yes	*(1) As documented in the audit, the document exists in DRAFT format; since OEM and DIT are separate reporting entities to City Administration it is beyond the scope of authority of the fire department to have any direct line responsibility for finalizing DIT contingency planning. Rather this function reasonably fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. That notwithstanding, Chief Thomas will meet with OEM leadership to discuss the audit findings specific to recommendations #5-7 to ensure their awareness that this shortcoming creates for the department as an end user. (2) It is more appropriate that OEM COOP Manager Schaal take the lead on ensuring the document DRAFT addresses all COBIT standards as addressed in The National Institute of Standards and Technology's (NIST), Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34 (as amended), prior to finalizing and 'signing-off' on the document and moving to the testing environment for closure and feedback/improvment.* *OEM Response* *OEM is working with DIT to complete their COOP Plan; however, the audit findings seem to reference a ITDR (Information Technology Disaster Recovery) Plan, not a COOP Plan. A COOP Plan focuses on maintaining essential functions during a disruption. An ITDR Plan specifies how to recover IT systems.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	SBC, COOP Manager, OEM Director & DIT Director		**31-Dec-11**
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
6	***Conduct testing and document the results of testing to examine the effectiveness of the COOP.***	Yes	*OEM will work with Fire in training and exercising their COOP Plan. Testing and documenting the results of this system would fall under the DIT's ITDR Plan and have no implication on the effectiveness of the Fire COOP Plan.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	COOP Manager, DIT Director		**12/31/2011**

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
7	*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.*	Yes	*OEM will work with Fire in training and exercising their COOP Plan. Testing and documenting the results of this system would fall under the DIT's ITDR Plan and have no implication on the effectiveness of the Fire COOP Plan.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	COOP Manager, DIT Director		12/31/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
8	*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.*	Yes*	*(1) DIT is its own, separate reporting, entity to City Administration. Accordingly, it is beyond the scope of authority for the fire department to have any direct line responsibility in finalizing DIT policy. Again, this function reasonably fits into a much broader organizational and business process planning responsibility. That notwithstanding, Chief Thomas will meet with the DIT Director to discuss the audit findings specific to recommendations #9 to ensure their awareness that this shortcoming creates for the department as an end user, and have them separately provide a written management response. (2) It is more appropriate that the DIT Director be held directly accountable for lack of general backup policy. DIT staff are more conversant in the multitude of decisions facing the issue of back up policy to include type (i.e., full, incremental, differential); storage sites (redundant geography); storage devices and desired data optimizations, managing and access to data repositories, etc. (3) Any key area responsibilities that translate from this policy directly to fire department staff shall be implemented as soon as reasonably possible.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	SBC, DIT Director		(2) 1/25/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
9	*Backup the FRMS data and servers on a daily basis.*	Yes*	The Fire database is backed up every day to disk. Daily tape backups for the system will be implemented by 1/31/11
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	DIT Director		31-Jan-11

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
10	*Create a formal process of recording all successful and unsuccessful backups to document the validity and reliability of the backup process.*	Yes*	Backup success and failure for tape backup is documented within the backup software for each backup session. This is part of the functionality of the software. We will add a method for documenting database backup failures by 3/1/11.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	DIT Director		1-Mar-11

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
11	*Create a formal process for performing a periodic tape restore testing and document the results showing both successful and unsuccessful backups from tape.*	Yes	We will add the test of backups on a quarterly basis to the backup policy by 3/1/11.
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	DIT Director		1-Mar-11

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
12	*Once the termination policy is established, enforce the procedures related to removing separated user access within the network and FRMS in a timely manner.*	Yes	*Develop the series of IT policies which will include account deactivation as discussed below in recommendation #21. In the absence of formal documents describing the action steps, both the Executive Administrative Assistant to the Fire Chief and Payroll Manager have been verbally directed to deactivate accounts in concert with internal department IT staff by the end of the pay-period following EE departure.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Executive Admin & Payroll Manager		7/1/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
13	*Work with the vendor to activate the password settings on FRMS.*	Yes	*While not minimizing the validity of the recommendation, until additional modules are optimized and populated with data, the strength of a users password is of lower concern because of the limited nature of sensitive information available. Most of the program wholesale features /capabilities (i.e., copying, printing reports, reformatting and design options , etc.) are already not available to the average user based on system privileges. As the dbase clean-up occurs we will work with the vendor to activate the "password expire" feature, which coupled with the strong password feature of SQL2008 adequately addrsses the recommendation.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	APA		3/30/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
14	*Upgrade the SQL database to SQL2008 as the current version (SQL 2000) does not support password functionality.*	Yes	*Build this recommendation in as a component part of the project schedule (implementation of modules and interfaces)*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Fire IT Support		3/30/2011
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION
	The Department was activity addressing the conversion. An upgrade to V10.1 was identifed as necessary for Win6. Data was tranferred over and then the platform "crashed." This coupled with of an OEMS mandate that required the submission of NEMSIS compliant patient medical records, much of the project scope was put on hold to achieve this regulatory requirement. All personnel were re-allocated to this function which delayed the implementation of remaining modules/interfaces and certain aspects of re-work to various in-place modules. Separately, the vendor was working with the department in Beta testing the Roster module. Because the implementation of Roster necessarily required upgrade to the Win6 environment, plans were in place to address the SQL database upgrade simulataneous with Roster roll out.		

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
15	*Perform testing to determine whether the Supervisor ID account can be disabled with no adverse effect to system maintenance and function.*	Yes	*Self Explanatory in recommendation, if no adverse effect to system performance, deactivate the account and ensure that all future practices limit the expsoure potential for reactivation.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Fire IT Support		2/1/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
16	***Remove GIS Analyst from the Supervisor group and add him to a group that is limited to accessing information relevant to his job responsibilities.***	**No**	*Because of the limited number of IT conversant staff within the department, a primary and two alternates who have ability to access, repair and administrate the dbase are necessary to 7/24 operations. The GIS analyst works very closely with the other two IT positions. If and when recommendation #2 is implemented, we can consider deactivating the second alternate.*
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Not Applicable		**Not Applicable**
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
17	***DIT_NT4_Admins group has administrative access to the FRMS database server. Restrict DIT_NT4_Admins group members to the Network Engineers team.***	**Yes**	*Self Explanatory in recommendation, if no adverse effect to system performance, activate the recommended restriction and ensure that all future practices limit the expsoure potential for reactivation.*
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	DIT Director		**2/1/2011**
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
18	***Upgrade the existing fire suppression system to have both gaseous and water based (pressurized dry pipes) fire suppression systems.***	**No**	*(1) DIT is its own, separate reporting, entity to City Administration. Accordingly, it is beyond the scope of authority for the fire department to have direct line responsibility in upgrading existing fire suppression systems under DIT purview. This function reasonably fits into a much broader organizational and business process planning responsibility. *That notwithstanding, Chief David Creasy (Fire Marshall) will meet with the DIT Director to discuss the audit findings specific to recommendation #19 to ensure awareness that this shortcoming creates for the department as an end user, and have them separately provide a written management response. (2) It is more appropriate that the DIT Director be held directly accountable for condition of the existing fire supression system and any shortcomings contained therein. (3) The U.S. Environmental Protection Agency (US EPA) encourages the use of non-ozone depleting fire suppression agent alternatives. Accordingly, the COR (in alignment with the established Focus areas of environmental friendliness) should carefully evaluate the cost/risk benefit of todays gaseous technology: Carbon Dioxide, Inergen®, FE – 227, ENCARO-25 Aerosol and Aero K. Each of these systems vary with respect to: global warming potential and/or ozone depletion potential; piping and floor space concerns; cleaning/venting requirements post activation; air integrity test room requirements and present potential toxicity to non-evacuated personnel. These considerations should place this audit recommendation on the City CIP plan.*
			DIT RESPONSE: *This is a two phase water based fire suppression system. Phase one fills the pipes, phase 2 allows the sprinkle. This is standard in major datacenter to include Oracle. This is not a valid finding and should be removed. AC's have been installed and are operational.*
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	DIT Director		**Not Applicable**
#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
19	***Continue phased replacement and upgrades to the major heating, air conditioning, ventilation, administrative space and electrical system in the Data Center as per the Capital Improvement Project.***	**No**	*See Above.*
	TITLE OF RESPONSIBLE PERSON		**TARGET DATE**
	Not Applicable		**Not Applicable**

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
20	*Establish a formal written security policy outlining the approval requirements for granting, modifying and removing access to FRMS. 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.*	Yes	*The department acknowledges that the presence of security policies represents the foundation of an organizational security strategy, and subsequently self disclosed during the initial stages of the audit, our acknowlegment of deficiency. The department is addressing a comprehensive series of IT policies covering commonly addressed issues including but not limited to: Acceptable Use, Passwords, Backup, Network Access, Incident Response, Remote Access, Virtual Private Network (VPN), Guest/Vendor Access, Wireless, Third Party Connection, Network Security, Encryption, Confidential Data, Data Classification, Mobile Device, Retention, Outsourcing, Physical Security, Change requests, Periodic Review/Athuntication of User Access and Software/Program Upgrades. In concert with policy development is the inclusion of developing standardarized department forms addressing common IT focus issues including, but not limited, to: Policy Acknowledgement, Security Incident, Notice of Policy Noncompliance, Account Setup Request, Guest Access Request and Request for Policy Exemption. All policy statements and developed forms will address documentation and record retention requirements. We recognize the value of "least privilege" concept and will ensure consideration during development.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	SBC		5/30/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
21	*Develop policies and procedures requiring the use of logical access authentication controls through the assignment of unique user IDs and strong passwords for all FRMS application users.*	Yes	*See Recommendation #20 Action Steps above.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	SBC		5/30/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
22	*Develop policies and procedures for managing changes including minor application changes, major application changes and software releases. This should include procedures for testing and receiving proper authorization and are supported by a change request document.*	Yes	*See Recommendation #20 Action Steps above.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	SBC		5/30/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
23	*Periodically review the user access to FRMS and the database.*	Yes	*See Recommendation #20 Action Steps above.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Fire IT Support		5/30/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
24	*Document the review results and their resolution.*	Yes	*See Recommendation #20 Action Steps above.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	APA		5/30/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
25	*Document the data interfaces with the outbound (i.e. submitting) and inbound (i.e. receiving) systems. The documentation should include at a minimum, the following items:* *• Data Elements contained within the interface;* *• Frequency of the interface;* *• Volume of transactions flowing through the interface;* *• Individual responsible for the operation of the data interface;* *• High-level business purpose for the interface;* *• High-level technical design description or diagram for the steps in the interface process, and;* *• Integrity of the data.*	Yes*	*(1) The department FRMS interfaces with two (2) external systems: OEMS and VA Fire Programs specific to NEMSIS V2.1 and NFIRS V5.0 (as amended/adopted). Each regulatory agency is very specific to inclusion of data elements, interface frequency, high-level business and technical design descriptions. The volume of transactions is defined by call volume in any given reporting period (although rarely varies by more than ± 5%). Accordingly, the vast majority of the audit recommendations are already in place. The remaining items: responsible individual will be addressed in policy development as described above in recommendation #20, the integrity of the data presents a separte departmental challenge and is addressed separately. (2) Data Integrity controls -- department wide training addressing this recommendation is planned throughout calendar year 2011. Training will occur over all modules, department wide at various user levels: input, review, QA/QI, benchmarking/reporting. Comprehensive training manuals will be developed for each user level (offered as an example is the attached NEMSIS manual).*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	SBC		12/3/12011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
26	*Implement change management procedures to ensure that all application changes and upgrades are approved, tested and documented prior to implementation.*	Yes	*See Recommendation #20 Above.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	SBC		5/30/2011
	IF IN PROGRESS, EXPLAIN ANY DELAYS		IF IMPLEMENTED, DETAILS OF IMPLEMENTATION

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
27	*Work with the FRMS vendor to determine if NFPA fire codes can be uploaded instead of keying them into FRMS.*	Yes*	*The department will explore (and if appropriate implement the) use of automated text insertion. This will reduce the dependency upon manual process and create a higher confidence in data integrity. This will be explored during the incident module clean-up and during the building of business validation rules into NFIRS reporting.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	APA		12/31/2011

#	RECOMMENDATION	CONCUR Y-N	ACTION STEPS
28	*Create an automated interface with the Proval system to import properties information.*	No	*Prior experience has demonstrated the Proval system to be an unreliable source of property information, which reduces data integrity during NFIRS reporting within the incident module. Until the Proval system reaches higher reliability with regard to accuracy and inclusion of all addresses/businesses the resultant output does not meet department business objectives and reporting.* *Audit Response:* *Fire should address this recommendation after Proval system reaches higher reliability with regards to data.*
	TITLE OF RESPONSIBLE PERSON		TARGET DATE
	Not Applicable		Not Applicable