



**GARLAND**

---

**INTERNAL AUDIT**

# **Financial Management Interfaces Audit**

**Craig Hametner, CPA, CIA, CMA, CFE**  
City Auditor

**Prepared By**

**J.Christian Thony**

**IT Audit Analyst**

**INTERNAL AUDIT DEPARTMENT**

**March 20, 2012**  
**Report 201103**

# Table of Contents

	<u>Page</u>
Authorization	1
Objective	1
Scope and Methodology	2
Overall Conclusion	2
Background	3
Management Accomplishments	12
Opportunities for Improvement	13
Glossary	18

## **Authorization**

We have conducted an audit of the Financial Management System Interfaces Audit. This audit was conducted under the authority of Article VII, Section 5 of the Garland City Charter and in accordance with the Annual Audit Plan approved by the Garland City Council.

## **Objective**

The objective of this audit is to evaluate the Financial Management System (FMS) interfaces for accuracy, internal controls, and efficiency. The assertions of this audit are completeness and accuracy of data transfer. To adequately address the audit objective, the sub-objectives were tested as follows:

1. All primary computing systems and network environments should have adequate documentation to describe their structure and operation.
2. All data transfers should be reconciled and reviewed for completeness, timeliness, and accuracy.
3. The IT department should utilize performance measurement and tuning, system availability, and capacity planning tools and utilities to ensure ongoing optimization and controls supporting business processes.
4. The IT department should have a method for logging transfer errors and the corrective actions taken to resolve them.
5. Appropriate procedures should be in place for setting alarms and logging entries for critical events. A procedure should also be in place to review the log files on a regular interval.
6. Scheduler operations should be controlled to ensure only authorized jobs are executed and that a proper job sequence is defined.
7. Critical systems and data ownership responsibility should be assigned for the City's applications and system data.
8. User access levels should be reviewed on a scheduled basis to ensure proper authorization.
9. A procedure should be in place to ensure the involvement or notification of other operating departments in the implementation of new applications or system updates/patches to ensure changes are implemented seamlessly.

10. All problems should be documented and changes must be authorized by management prior to their installation in the production environment.
11. The number of people who can make changes to the system should be limited.
12. Firewall and perimeter security device administration should be performed.

### **Scope and Methodology**

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Information Technology controls were tested under the COBIT framework methodology.

We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This included compliance with directives, policies and procedures. Our audit period covered from 10/01/2010 through 09/30/2011.

While we report to the Mayor and City Council and present the results of our work to the Audit Committee, we are located organizationally outside the staff or line management functions we are auditing. Therefore, this Audit organization may be considered free of organizational impairments to independence to audit internally and report objectively to those charged with governance.

### **Overall Conclusion**

Out of the 13 interfaces tested, the Internal Audit (IA) department only noted one inaccurate import. The reconciliation mechanism however is designed to detect inaccurate records and allows the user to perform a total comparison between the source and imported data. This is a detection mechanism that mitigates the risk of inaccurate data entry if a follow-up is conducted on the noted deviation. In this instance the problem resolution went through the proper channels and has been resolved.

When it comes to the change management process we noted that the notification and problem resolution controls were operating effectively. However, we noted that there were no restrictions to limit developer access in the production environment in the design of these controls. The developer is also the implementer, custodian, and maintenance technician for the developed

applications giving him a full range of access. This design flaw is attributed to the staffing resource limitations at the Information Technology Services department. Nevertheless, the current design allows the risk of unauthorized changes being promoted into the production environment due to a lack of segregation of duties. Furthermore, the logical security access to critical files and resources does not enforce restrictions based on job responsibility. Information Technology Services security controls are not effectively designed.

From an efficiency and problem resolution perspective the IA department believes that the current controls provide reasonable assurance that data is imported accurately and that problems are solved on a timely basis.

From a logical security perspective surrounding segregation of duties and access restrictions based on job responsibility the IA department believes that the current controls do not provide reasonable assurance that unauthorized changes are made into the production environment.

## **Background**

The City of Garland relies on data located in the Financial Management System in order to issue its annual financial statement. The data located therein comes from multiple sources scattered around the City. Data extraction from these systems is performed through the use of interface middleware applications.

An interface is a method which allows different incompatible systems to communicate with each other. For instance, an operating system may interface with pieces of hardware and applications. The interface performs data conversion, reformatting, import, and export. At the City of Garland, the Financial Management System interfaces with several entities. These entities are categorized as follows:

### **Internal Entities**

Internal entities are comprised of City of Garland departments. These departments have independent systems that gather critical financial data. This data is then manually retrieved on a periodic basis depending on the frequency of the imports.

- Human Resources
- Customer Service
- Code Compliance
- Housing

- Municipal Court
- Parks & Recreations
- Library

### **External Entities**

The Financial Management System interfaces allow the exchange of data with external entities. Financial information is extracted from and relegated to these parties. Vendor and employee payments are reconciled. Direct deposit through the Automated Clearing Houses financial network, banking, and payroll data comprise the totality of these transactions.

- JP Morgan Chase Bank

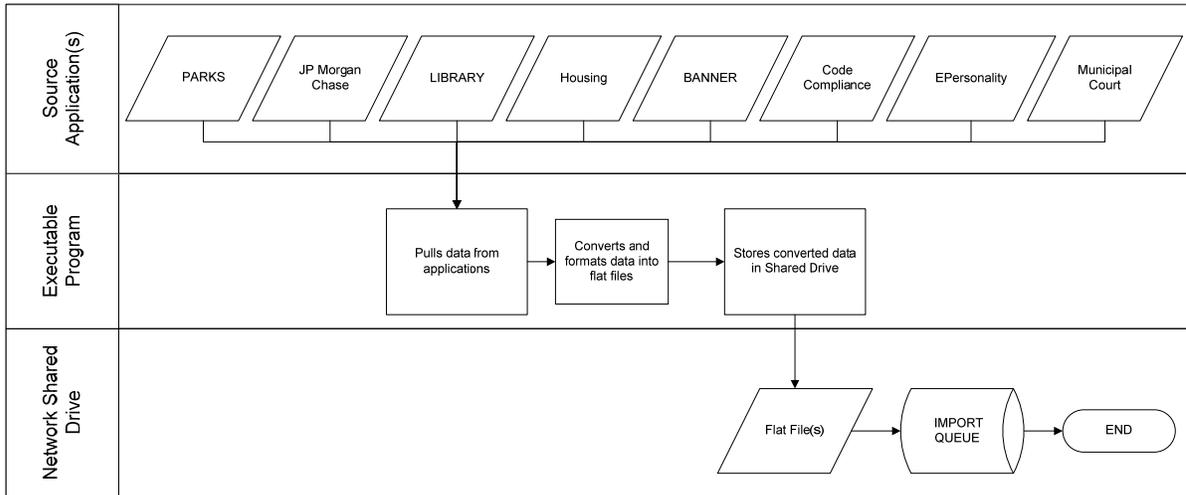
### **Data Processing**

Data Processing requires two separate steps prior to being transferred into the Financial Management System. The executable programs are first ran in order to perform the initial extraction and conversion. The Financial Management System (FMS) Report Interface enables the actual import and reconciliation of the source data. The Interface at the City of Garland can then be considered as fragmented into two separate steps Executable Programs and FMS Report Interface.

***Executable Programs*** (*Exhibit 1*) initiate the process of extracting data from source application systems and reformatting them into flat files. The flat files are then stored on the shared drive. The data then becomes available and ready to be manually imported into the Financial Management System.

## Exhibit 1

### Executable Programs

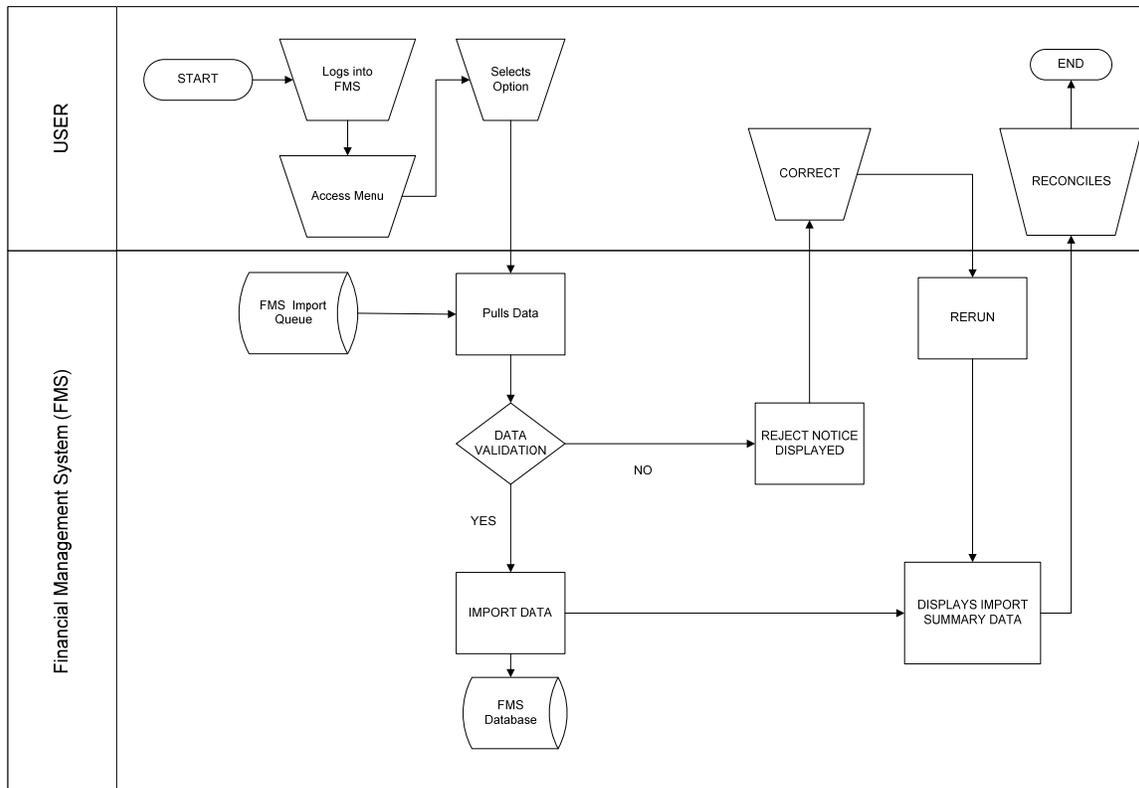


Source: Internal Audit.

***Financial Management System Report Interface (Exhibit 2)*** is the manual process initiated by Finance users. In this process, data is extracted and validated prior to final import. A summary of imported data report will be generated by the user in order to perform data reconciliation for completeness and accuracy.

## **Exhibit 2**

### **Financial Management System Report Interface**



Source: Internal Audit.

### **Rex Control Management System**

The REX Control Management System (CMS) is utilized in order to perform user access provisioning to the multiple FMS interfaces. The CMS is equipped with features such as user impersonation and a password authentication access control. Access to these various interfaces is restricted at different levels.

- **Local Level:** In order for users to be able to utilize the interface applications they have to be installed on their local machines. Without accessibility to the interface executable files users will not be able to import/export data to and from the Financial Management System.
- **Control Management System Level (Exhibit 3):** Just because you can see the executable file does not mean that you can run it. In order for a user to be able to execute these files they will need to be setup inside of the REX Control Management System. User access privileges to specific applications are assigned within the CMS.

### Exhibit 3

<b>Appid</b>	<b>Connectionnotes</b>	<b>Functionality</b>	<b>Description</b>	<b>Entity</b>
AP575T	AP Domestic Issues FTP Download Destination	The application is executed from the desktop of the Sr Financial Accounting Technician in Finance	The AP575T "Monthly Cleared Domestics" process is created to download the cleared AP checks from JPMorgan Chase and import them into the Cayenta finance system.	JP Morgan Chase
AP970T	Foreign Issues Interface for Reconciliation	The application is executed from the desktop of the Sr Financial Accounting Technician in Finance	The AP970T "Monthly Cleared Foreign" process is created to download the cleared Payroll checks from JPMorgan Chase and import them into the Cayenta finance system.	JP Morgan Chase
APChequeImport	Import destination for chequescribe files copied down from Finance	Execution of the AP Check Import application directs the user to import the data from their Cayenta AP print spool queue .	This process retrieves Account Payable detail from the Cayenta financial system into ChequeScribe in order to print checks.	Finance
APFTP	APFTP	This profile is executed from the desktop of the Accounting Technician or the Accounting Supervisor, through the All-Purpose FTP application	Creates a file from Indus Utility System to upload into Cayenta AP Foreign Subsystem Interface which is used to create Utility Refund Checks.	Customer Service
BNRACTPULL	Primary connection string for Weekly Banner account file build for Fidelity Express and Aperta	This profile is executed from the desktop of the Accounting Technician or the Accounting Supervisor, through the All-Purpose FTP application	Creates a file from Indus Utility System to upload into Cayenta AP Foreign Subsystem Interface which is used to create Utility Refund Checks.	Customer Service

<b>Appid</b>	<b>Connectionnotes</b>	<b>Functionality</b>	<b>Description</b>	<b>Entity</b>
CRMCCGL	CRM Cash Receipt / GL Interface	The Code-side extract, through this interface, is run by the Court Services Supervisor or the Court Services Supervisor in the Code Enforcement department. The finance-side import of the extracted data is run, through this interface, by the Accounting Supervisor in Finance.	Creates a file from the Code Enforcement system to upload into the Cayenta Interface Entry Level Import which is used to upload GL entries from the Code system.	Code Enforcement
HOUSEPROAP	Test / VB6 version of HOUSEPROAP ONLY!	The Housing-side extract, through this interface, is run by the Housing Fiscal Supervisor in the Housing department. The finance-side import of the extracted data is run, through this interface, by either the Accounting Technician or the Accounting Supervisor.	Creates a file from Housing's Happy HousingPro system to upload into Cayenta AP Foreign Subsystem Interface which is used to create Housing payments to landlords.	Housing
HRAP	P2K connection	Interface extracts data from Hi-Line payroll system such as deductions and summarizes data as needed by the Payroll Technician. Once data is ready to be imported in to Cayenta, the Accounting Technician or the Accounting Supervisor are notified via e-mail.	Creates a file from Payroll's P2K system to upload into Cayenta AP Foreign Subsystem Interface which is used to create payments to various payroll related vendors. (ie: child support payments to the Attorney General).	Human Resources
MCAP	Municipal Court database	The Municipal Court-side extract, through this interface, is run by the Court Services Supervisor. The finance-side import of the extracted data is run, through this interface, by either the Accounting Technician or the Accounting	Creates a file from the Municipal Court (CourtHouse) system to upload into Cayenta AP Foreign Subsystem Interface which is used to create bond refund checks.	Municipal Court

Appid	Connectionnotes	Functionality	Description	Entity
		Supervisor.		
PARKSGL	Primary data connection to Parks CLASS database for GL interface	Both the extract and import sides of the GL data interface are handled by Finance, supported by data provided by Parks.	Creates a file from the Parks (CLASS) system to upload into the Cayenta Interface Entry Level Import which is used to upload GL entries from the Park system.	Parks
PARKSAP	Primary data connection to Parks CLASS database for AP interface	Both the extract and import sides of the GL data interface are handled by Finance, supported by data provided by Parks.	Creates a file from the Parks (CLASS) system to upload into the Cayenta Interface Entry Level Import which is used to upload GL entries from the Park system.	Parks
PAYISSUES	Payroll Issues	File is exported to JPMChase bank through user-executed JPMC-provided web-based upload interface.	This process allows the City to extract JP Morgan payments from its website it is a precursor to the Foreign and Domestic check reconciliation process.	JP Morgan Chase
SymphonyAP	AP impersonation entry.	Data is extracted by users the Management Assistant and the Accounts Payable Technician, through the interface, from files release from the Symphony system. The finance-side import of the extract data is run, through this interface, by either the Accounting Technician or the Accounting Supervisor.	Creates a file from the Library Symphony system to upload into Cayenta AP Foreign Subsystem Interface which is used to create payments to various Library related vendors.	Library

Source: REX Control Management System (Appid, Connectionnotes, Functionality) and AP Accounting Supervisor (Description, Entity).

- **Connection Strings Level:** Connection strings are located within the REX database where access parameter values are defined and stored. The several aforementioned “*appids*” represent the different applications who call on these predefined functions.

### **Paywiz**

This process allows the City of Garland to issue direct deposit payroll payments to its vendors. It is now currently managed by the REX Control Management System. This process extracts information from the Accounts Payable module of the Financial Management System and exports it to JP Morgan Chase Bank through Automated Clearing Houses (ACH) electronic network in order to provide vendor payments.

### **Change Management**

In order to ensure an acceptable level of customer support, Information Technology Services (ITS) has established consistent and efficient processes and procedures, using technology and computing resources that are outlined and defined within this Service Level Agreement.

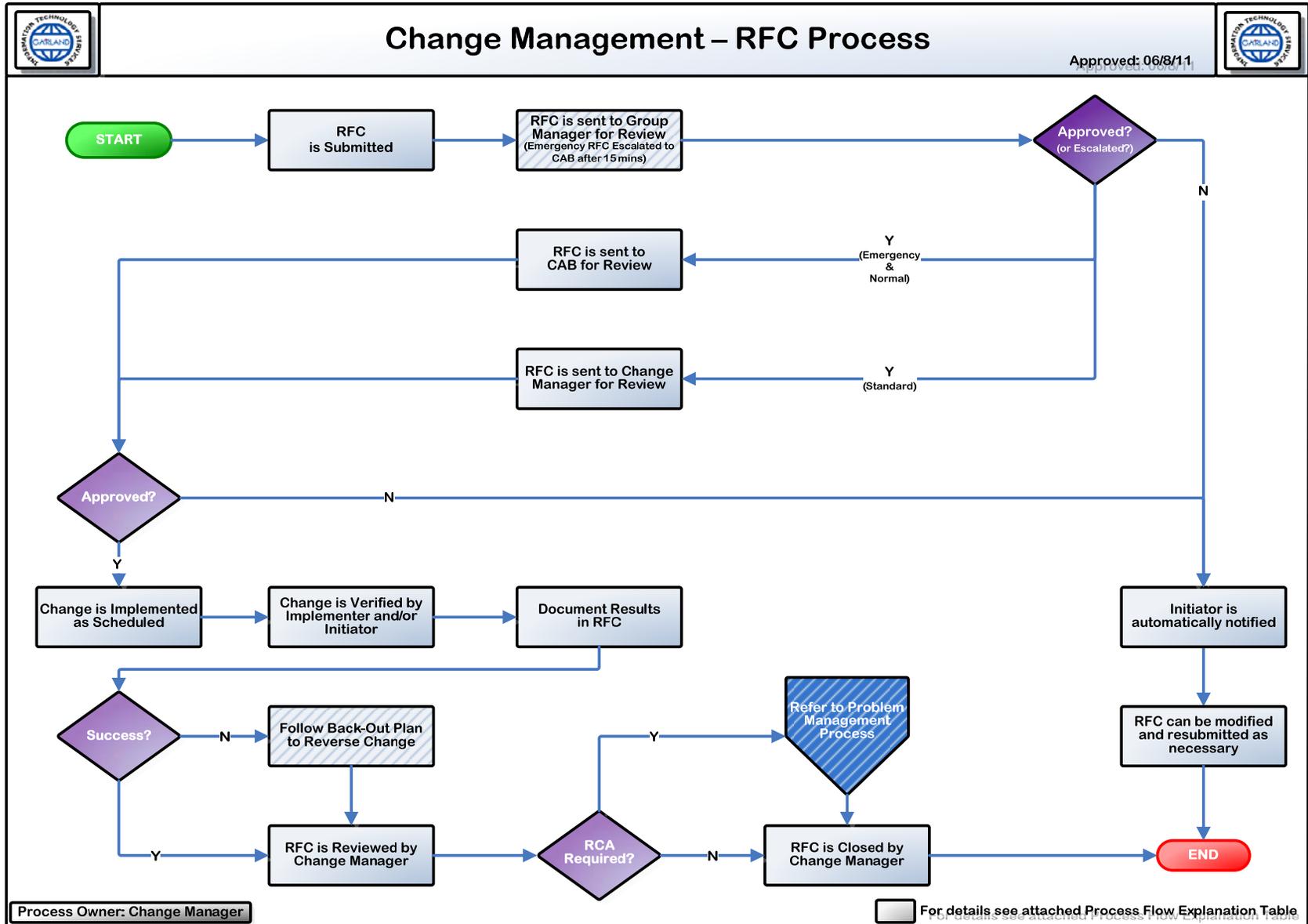
The efficient operation and service of these products require that ITS and its customers share and understand support procedures, roles and responsibilities, lines of communication, and expectations. Changes are initiated and tracked by the Service Desk. User requests to the Service Desk are documented and notifications are sent via email when the requests have been logged and assigned a work order number. Another email notification will be sent to user upon resolution of their requests.

The City of Garland maintains a Change Management Policy included in the ITS Standard Operating Procedures (OPS) manual. The procedure documents the Request for Change (RFC) process which requires three levels of approval prior to a change being initiated for critical projects (*exhibit 4*).

For requests that become projects. A resolution will be provided within 30 days by closing the ticket and providing a project plan number. Microsoft Project will be utilized to manage the project which may be subject to review from the Change Advisory Board if changes will be made to the production systems not in the testing environment.

Executable files or interface programs that are built in the .Net environment are equipped with the click-once automatic upgrade which allows the applications to look for any published updates for their setup files. This allows changes to be automatically disseminated on local machines automatically once new updates are published.

### Exhibit 4



Source: ITS-Standard Operations Manual Approved on 06/08/2011

## **Management Accomplishments**

**IT is very concerned with processes, security and integrity of data in any application managed by the IT team. A few of the accomplishments IT made is:**

1. Discontinue the use of generic logins to Active Directory.
2. Discontinued use of generic logins to applications.
3. Databases users must have a named login that expires every 90 days.
4. A separation of programmer duties document has been presented to the CIO for approval.
5. User Entitlement review will include a review of IT User access for 2012.

## Opportunities for Improvement

During our audit we identified certain areas for improvement. Our audit was not designed or intended to be a detailed study of every relevant system, procedure, and transaction. Accordingly, the Opportunities for Improvement section presented in this report may not be all-inclusive of areas where improvement might be needed.

Finding #	Condition (The way it is)	Criteria (The way it should be)	Cause (Difference between condition & criteria)	Effect (So what?)
1 (obj. 2)	The HouseProAP interface system inaccurately imported \$216.98 as opposed to \$2169.80. This was a result of a decimal conversion error in the logical coding of the interface application.	The HouseProAP interface accurately imports data into the Accounts Payable table located in the Financial Management System.	Data was imported at the wrong decimal point because of a logical failure in the HouseProAP interface.	System will import inaccurate data into the Financial Management System. Inaccurate payments may be processed.
Recommendation	Management Response	Action Plan	Implementation Date	Auditor's Comment
Interface functionality for accuracy should be tested and resolved by the Information Technology Services department.	Concur with findings	This was resolved upon discovery.	Dec 12, 2011	

<b>Finding #</b>	<b>Condition (The way it is)</b>	<b>Criteria (The way it should be)</b>	<b>Cause (Difference between condition &amp; criteria)</b>	<b>Effect (So what?)</b>
2 (obj. 7)	No evidence was available to confirm that user access levels were reviewed periodically for Developers, Change Migrators, and application Maintenance Technicians.	User access levels are reviewed on a regular basis to ensure authorization is appropriate and up to date.	No standard procedures have been established to ensure that user access level reviews are performed on a periodic basis.	A lack of periodic review of access levels to data files could expose the City to unauthorized access to applications and system data.
<b>Recommendation</b>	<b>Management Response</b>	<b>Action Plan</b>	<b>Implementation Date</b>	<b>Auditor's Comment</b>
User access levels at the domain, critical system, and database-levels should be reviewed on a regular basis to ensure authorization is appropriate and up to date. The evidence of review should be retained.	Concur with Finding	IT will undergo a review of user access levels with the User Entitlement review that occurs annually. This review will be done in May of each year.	May 2012	

<b>Finding #</b>	<b>Condition (The way it is)</b>	<b>Criteria (The way it should be)</b>	<b>Cause (Difference between condition &amp; criteria)</b>	<b>Effect (So what?)</b>
3 (obj. 9)	Internal Audit is unable to obtain evidence that testing was performed and retained prior to change being implemented into production.	Change management policies and procedures provide for changes' authorization, approval, notification schedule, testing and monitoring.	This was a deviation from standard procedure. Evidence should have been retained for testing (performance, compatibility, and load). This was due to human error.	No formal authority to review and approve proposed system changes may result in improper changes impacting the production environment.
<b>Recommendation</b>	<b>Management Response</b>	<b>Action Plan</b>	<b>Implementation Date</b>	<b>Auditor's Comment</b>
Testing should be performed prior to implementation into the production environment. Evidence of testing should be retained.	Concur with Finding	There is a process in effect for this recommendation; however, it has not been strictly enforced. Managers who approve RFC must ensure the necessary testing documentation is included with the RFC upon approval. Submitters of RFC must be cognizant to include testing signoff from the user upon submitting RFC.	Immediately	

Finding #	Condition (The way it is)	Criteria (The way it should be)	Cause (Difference between condition & criteria)	Effect (So what?)
4 (obj. 6, 10)	<ul style="list-style-type: none"> <li>One (1) System Admin Account password is shared by entire Domain Admin Group which is comprised of eight individuals including two contractors.</li> <li>One (1) employee retired as of 12/31/2009 and still had access.</li> <li>Two (2) Developers have Full access from the development phase all the way the implementation and maintenance phase. No segregation of duties present.</li> <li>One (1) user has developer access without appropriate title and the ability to migrate changes into the production environment and modify the database instances.</li> <li>Five (5) users have no access to the development folder but can modify access into the production environment through the Finance interface folder</li> </ul>	<p>Access privileges to critical systems and ownership over the significant resources are appropriate based on the job responsibilities.</p> <p>Developers and testers should not promote codes into the production environment.</p>	<p>Access privileges to critical systems and ownership over the significant resources are not appropriate based on the job responsibilities.</p> <p>This design flaw is attributed to the staffing resource limitations at the Information Technology Services department.</p>	<p>Unauthorized access to City applications and systems could lead to loss destruction or unauthorized change of critical applications and data.</p>

	<p>and the database REX entries.</p> <ul style="list-style-type: none"> <li>Two (2) accounts have development access and can modify files in the production environment.</li> </ul>			
<b>Recommendation</b>	<b>Management Response</b>	<b>Action Plan</b>	<b>Implementation Date</b>	<b>Auditor's Comment</b>
<ul style="list-style-type: none"> <li>The job responsibilities of Developers should enforce proper segregation of duties preventing them from promoting code into the production environment.</li> <li>Retired user accounts should be removed from the domain.</li> <li>Critical access should be restricted based on job responsibilities.</li> </ul>	<ol style="list-style-type: none"> <li>Concur with Finding</li> </ol>	<ol style="list-style-type: none"> <li>The domain administrator password has been changed. The password was created by two individuals and sealed in an envelope stored in a safe. No one person knows the domain administrator password.</li> <li>Account has been disabled and will be removed from the domain.</li> <li>A document will be presented to segregate the duties of the programmers implementing change into production systems.</li> <li>The person in question was an intern and was granted rights the same as other programmers. The intern did help with the coding of interfaces</li> </ol>	<ol style="list-style-type: none"> <li>Completed 2/02/12</li> <li>Account disabled – Completed 2/02/12. Account removed from domain –February 2012</li> <li>March 31, 2012</li> <li>Completed 2/3/2012</li> <li>No action required</li> <li>Completed 2/3/2012</li> </ol>	

		<p>and application while with the city. In the future rights granted to interns will be reviewed and scrutinized. This person is no longer an intern with IT and all rights have been terminated.</p> <p>5. The group assigned to the Finance-interface folder was given full access to the folder when in fact the group should have only been given read access. By changing the access rights to the folder users will not be able to change files in the folder. Ticket # 138966 has been issued to correct this problem. No users have access to the Development directory. No user can modify access into the REX Database.</p> <p>6. The App-Dev group is the group that gave access to the two accounts. These accounts have been removed from the group.</p>		
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

## Glossary

- **Logical Security:** consists of software safeguards for an organization's systems, including user identification and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation. It is a subset of computer security.
- **Middleware Application:** computer software component or people and their applications. The software consists of a set of services that allows multiple processes running on one or more machines to interact.
- **Flat Files:** plain text or mixed text and binary file which usually contains one record per line or 'physical' record (example on disk or tape). Within such a record, the single fields can be separated by delimiters, e.g. commas, or have a fixed length. In the latter case, padding may be needed to achieve this length.
- **Source Application:** Application or process where the data is originating from. The source of the imported data.
- **Impersonation:** Logical access capability that enables a user to have access privileges of another account.
- **Click-Once Automatic Upgrade:** The ability to for executable files built in a .Net environment to check for automatic version updates and self-update.
- **Password Authentication:** Logical access restriction that requires the use of a password in order to validate the identity of a user and grant them access to a system.
- **Automated Clearing Houses (ACH):** is an electronic network for financial transactions in the United States. ACH processes large volumes of credit and debit transactions in batches. ACH credit transfers include direct deposit payroll and vendor payments.
- **Domain:** is an identification string that defines a realm of administrative autonomy, authority, or control in the Internet. In the context employed in this report it is used to reflect the City of Garland's internal network.