



GARLAND

INTERNAL AUDIT

Date: September 24, 2013

To: Honorable Mayor Athas
Members of the City Council
Members of the Audit Committee

From: Craig Hametner, City Auditor

Subject: Financial Management Interfaces Audit Follow-up

This is a follow-up of the report “Financial Management Interfaces Audit” issued on March 20, 2012. The original audit included testing of procedures assessing management controls, such as reviewing segregation of duties, checks and balances, accurate utility billing, proper revenue reporting, compliance with laws, regulations, City ordinances, and professional service agreements. The follow-up audit was not intended to be a detailed study of every relevant system, procedure, and transaction.

We performed this follow-up 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.

This audit follow-up was conducted 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our previous recommendations.

To verify that recommendations had been implemented, we performed the following:

Audit Follow-Up

Finding #1

Condition (The way it is)

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.

Recommendation

Interface functionality for accuracy should be tested and resolved by the Information Technology Services department.

Management Response

Concur with findings.

Action Plan

This issue was resolved upon discovery.

Implementation Date

December 12, 2011

Follow-up

We selected four monthly housing statements between July 2012 and May 2013. We verified the imported amount from the housing system matched the amount uploaded into the financial system.

Implementation

Fully Implemented

Finding #2

Condition (The way it is)

No evidence was available to confirm that user access levels were reviewed periodically for Developers, Change Migrators, and application Maintenance Technicians.

Recommendation

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.

Management Response

Concur with finding.

Action Plan

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.

Implementation Date

May 2012

Follow-up

We reviewed the 2013 user entitlement review signed off by the CIO to verify that access is reviewed for all of the IT staff.

Implementation

Fully Implemented

Finding #3

Condition (The way it is)

Internal Audit is unable to obtain evidence that testing was performed and retained prior to change being implemented into production.

Recommendation

Testing should be performed prior to implementation into the production environment. Evidence of testing should be retained.

Management Response

Concur with finding.

Action Plan

There is a process in effect for this recommendation; however, it has not been strictly enforced. Managers who approve an RFC must ensure the necessary testing documentation is included with the RFC upon approval. Submitters of the RFC must be cognizant to include testing signoff from the user upon submitting the RFC.

Implementation Date

Immediately.

Follow-up

Reviewed a random sampling of 8 change tickets. Verified the appropriate approvals and testing signoffs were included in the change ticket documentation.

Implementation

Fully Implemented

Finding #4

Condition (The way it is)

1. One (1) System Admin Account password is shared by entire Domain Admin Group which is comprised of eight individuals including two contractors.
2. One (1) employee retired as of 12/31/2009 and still had access.
3. Two (2) Developers have Full access from the development phase all the way the implementation and maintenance phase. No segregation of duties present.
4. One (1) user has developer access without appropriate title and the ability to migrate changes into the production environment and modify the database instances.
5. Five (5) users have no access to the development folder but can modify access into the production environment through the Finance interface folder and the database REX entries.
6. Two (2) accounts have development access and can modify files in the production environment.

Recommendation

- The job responsibilities of Developers should enforce proper segregation of duties preventing them from promoting code into the production environment.
- Retired user accounts should be removed from the domain.
- Critical access should be restricted based on job responsibilities.

Management Response

1. Concur with finding.
2. Concur with finding.
3. Concur with finding.
4. Concur with finding.
5. Concur with finding.
6. Concur with finding.

Action Plan

1. 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.
2. The account has been disabled and will be removed from the domain.
3. A document will be presented to segregate the duties of the programmers implementing change into production systems.
4. 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 and applications 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.

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.
6. The App-Dev group is the group that gave access to the two accounts. These accounts have been removed from the group.

Implementation Date

1. Completed 2/2/2012.
2. Account disabled – completed 2/2/2012. Account removed from domain – February 2012.
3. March 31, 2012
4. Completed 2/3/2012
5. No action required.
6. Completed 2/3/2012

Follow-up

Although there are three (3) recommendations listed for this finding, the follow-up for Finding #4 was performed by verifying the six (6) conditions to the corresponding management responses and action plan.

1. We verified the procedure by observing the process for securing and storing the domain administrator password.
2. We verified that user account access for a retired employee had been removed from the City network.
3. Documentation and system access was reviewed to verify that proper segregation of duties had been implemented for Developers in the IT Department.
4. We reviewed user access to verify proper access had been granted based on job responsibilities.
5. The user access rights were reviewed for two (2) users in Ticket #138966. One user no longer is an employee. The other user is an active employee and does not have user access rights to the REX database.
6. Two (2) user accounts were verified to ensure that access has only been granted to development.

Implementation

Fully Implemented