



**GARLAND**

**INTERNAL AUDIT**

# **Utility Systems Access Rights Audit**

**Jed Johnson, CGAP  
Interim City Auditor**

**Prepared By  
Melinda Milner, CISA, CISSP, CRISC  
Sr IT Auditor**

**November 25, 2013  
Report 201308**

# Table of Contents

	<u>Page</u>
Authorization .....	1
Objective, Scope and Methodology .....	1
Overall Conclusion .....	2
Background.....	2
Opportunities for Improvement .....	4
Exhibit A - Reliability of Computer Generated Data .....	12

## **Authorization**

We have conducted an audit of the Utility Systems Access Rights 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**

1. Determine the controls in place to ensure only authorized employees can access the Utility Systems.
2. Determine the controls configured for the Utility systems to enforce proper segregation of duties.
3. Evaluate third-party access to ensure adequate controls exist for vendors providing remote payment services.

## **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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of the audit is the current timeframe and Internal Audit (IA) audited access rights and segregation of duties for the Banner and iNovah utility billing applications. (See Exhibit A for reliability of computer generated data.)

To adequately address the audit objectives and to describe the scope of our work on internal controls, we reviewed the following:

- Obtain and reviewed IT and Utility billing system current policies and procedures (Obj. 1 & 2).
- Obtain and review third-party contracts. (Obj. 3)
- Obtained and verified third party provider documentation for PCI (Payment Card Industry) Validated Payment Application compliance certification. (Obj. 3)
- Obtained and verified the third party Service Organization Control (SOC) 2 Security, Availability, and Processing Integrity Audit Report for the Western Union/Speedpay system. (Obj. 3)
- Obtained and reviewed annual user access rights entitlement review for utility billing system applications for all Managing Directors. (Obj. 1 & 2)

- Reviewed security group access rights for Customer Service employees for the Banner application. Reviewed entire population of Customer Service employees' user access for the iNovah application. (Obj. 1 & 2)
- Obtained and reviewed utility billing system's operating system and database user accounts for appropriateness. (Obj. 1 & 2)
- Verified administrative rights were granted to proper personnel. (Obj. 1)
- Created and assessed job matrices to review for proper segregation of duties for Customer Service employees. (Obj. 2)
- Verified user passwords are encrypted for the utility billing system. (Obj. 1)

Any deficiencies in internal controls that are significant within the context of the audit objectives and based upon the audit work performed are stated in the Opportunities for Improvement section starting on page 4.

### **Overall Conclusion**

1. Customer Service security groups have overlapping access to accommodate the business need to rotate as needed in customer-facing roles. Periodic monitoring is not performed to ensure access permissions are appropriate. (Obj. 1 & 2)
2. The Annual User Entitlement Report provides the user and security group and does not reflect a detailed listing of user access rights for the Banner utility billing application. The iNovah cashier application was not included in the annual user access entitlement review. (Obj. 1 & 2)
3. A segregation of duties issue exists for an IT employee with the dual job responsibilities of Oracle DBA and Senior Systems Information Analyst roles. (Obj. 2)
4. Terminated, temporary and duplicate accounts were not disabled in a timely manner when no longer needed. (Obj. 1 & 2)
5. We reviewed the third-party agreements and (SOC) 2 audit reports for the remote payment vendor and no issues were found. (Obj. 3)

### **Background**

Utility Customer Service provides meter reading, billing and collection services for all city utilities. These utilities include Garland Power & Light, Garland Water Utilities, Environmental Waste Services and Stormwater Management. This does not include natural gas service which is provided by Atmos Energy.

Two applications are utilized to support the Utility Customer Service Department. The Banner application is used for customer account maintenance and billing. Banner was installed in 2007 and has approximately 314 users. The iNovah application is used by the cashiers to process customer payments, credits and

refunds. The iNovah application was installed in 2007 and has 31 users. The City IT Department supports both systems.

Utility Customer Service customers have access to two downtown Garland Customer Service locations:

Charles E. Duckworth Utility Services Building  
217 N Fifth Street (across from City Hall)

Garland Utility Payment Drive Thru and Drop Box  
717 State Street (corner of State and Glenbrook)

Utility: customers can also conduct business online via the [garlandutilities.org](http://garlandutilities.org) website. Online options include

- Online bill pay
- Account management
- Request utility services
- Set up E-bill
- Energy efficiency and water conservation programs

Other convenient payment options available for paying a utility bill include the following:

- Credit/Debit card via phone
- Automatic Bank Draft
- Mail

## 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 #1 (Obj. 1 & 2)-Customer Service

#### Condition (The way it is)

Customer Service security groups have overlapping responsibilities in order to meet the business need to rotate employees for customer service job responsibilities.

#### Criteria (The way it should be)

Segregation of duties should exist to grant user access on a least privilege basis or implement mitigating controls.

#### Effect (So what?)

Overlapping user access may give a user(s) more access to engage in inappropriate activities in the billing/collection system.

#### Cause (Difference between condition & criteria)

Management has created the overlap in user access to accommodate the business need in providing their customer uninterrupted customer service.

#### Recommendation

As Customer Service employees have overlapping access in Banner and iNovah, it is recommended that management perform periodic monitoring by reviewing user activity reports (adjustment reports, red flag reports, etc.) to ensure accuracy and appropriateness of customer service transactions/activities.

#### Management Response

Concur. Customer Service management will conduct an annual review of Payment Center employee access rights in Banner and iNovah, plus periodic reviews of user activity reports.

#### Action Plan

Department will utilize a process similar to the one recently conducted by Internal Audit to ensure user access is as limited as possible. Customer Service will work to ensure the following: identify users assigned to all Banner Security Groups by using report compiled by IT staff, review the Banner forms that each group is permitted to access and verify that access is required for job duties, confirm that employees are assigned to Security Groups that are appropriate to each employee's job duties, identify iNovah security groups using iNovah Group Security Report compiled by IT staff, review the iNovah forms that each group is permitted to access and verify that access is required for job duties, confirm that employees are assigned to Security

Groups that are appropriate to each employee's job duties.

**Implementation Date**

At the end of each year (December).

## Finding #2 (Obj. 1)-ITS

### Condition (The way it is)

An annual user access entitlement report is generated by IT for several applications used Citywide. The report is distributed to all Managing Directors for review and sign-off for appropriate access. The 2013 user entitlement review report was missing 36 user accounts for Banner users for Customer Service and other City Department users.

### Criteria (The way it should be)

User entitlement reports should be reviewed to verify all users of a department are included in the annual review.

### Effect (So what?)

Without a detailed user access review for the Banner application, unauthorized access may not be captured.

### Cause (Difference between condition & criteria)

The report did not pull all of the users for the Customer Service group and other City Department groups.

### Recommendation

Review the process for generating user entitlement reports to ensure all user accounts are captured.

### Management Response

IT Management Concur. Since reports pulled from the application were matched against the HR system, temporary and contract workers were missed because they are not in the cities HR system. In order to ensure all workers (temporary and contractor) are accounted for, IT has created a User Entitlements database to track every account created for applications. This new database will be utilized for the 2014 User Entitlement report to Managing Directors.

### Action Plan

Track all user accounts created for application in a User Entitlement database. When users are no longer required to have rights an application they will be removed from the application appropriately and marked as disabled in the User Entitlement database.

### Implementation Date

The User Entitlement report is created in May and distributed to Managing Director the first week of June.

### Finding #3 (Obj. 1)-ITS

#### Condition (The way it is)

The annual user access entitlement reviewed is generated for several applications used Citywide. IT generates a report by user account and security group.

1. The individual user access for the assigned security group is not listed in the report.
2. There currently is not an annual user access review for the iNovah application.

#### Criteria (The way it should be)

User access reviews should be performed by reviewing user accounts, security groups and access rights granted within the security group.

#### Effect (So what?)

1. Without a full review of access rights, management is unable to verify that appropriate access has been granted for user accounts.
2. Unauthorized or inappropriate activities may go unnoticed.

#### Cause (Difference between condition & criteria)

1. The user entitlement report only pulls the username and security group.
2. An annual user entitlement review is not being performed.

#### Recommendation

1. The annual user entitlement review should be expanded to include the user access rights with the security groups for all Banner users.
2. The iNovah application should be added to the annual user entitlement review.

#### Management Response

Management Concur on 1 and 2.

#### Action Plan

1. ITS will create a comprehensive rights document for all applications in the User Entitlement report and publish either on the city "G:" drive or on the COGnet site for all Managing Director to access.
2. Inovah User Entitlement will be included in the 2014 User Entitlement report

#### Implementation Date

May 2014 before the next User Entitlement report is issued.

**Finding #4 (Obj. 1 & 2)-ITS**

**Condition (The way it is)**

During the audit, a segregation of duties conflict was noted with the overlapping role of Oracle DBA and Sr Information Systems Analyst role. Since then an employee has been hired to perform the Information Systems Analyst support role. Training/transition is currently underway to split the two roles.

**Criteria (The way it should be)**

Segregation of duties should exist between application and database support for the Banner utility system.

**Effect (So what?)**

Unauthorized or inappropriate activity may occur due to the lack of segregation with the two support roles.

**Cause (Difference between condition & criteria)**

Limited IT resources have caused the overlap of support for the application and database.

**Recommendation**

Ensure application access permissions are removed for the Oracle DBA at the completion of training and transition.

**Management Response**

Management Concur.

**Action Plan**

There will continue to be an overlap of duties until the system analyst has completely trained.

**Implementation Date**

IT estimates that training will be completed on or before May, 2014.

## Finding #5 (Obj. 1)-ITS

### Condition (The way it is)

Upon review of application and database user accounts, we found the following:

1. A temporary employee no longer working in the Customer Service department still had access to Banner.
2. Five users had duplicate user accounts.
3. A terminated user account was active in the iNovah application.
4. A test account was active that was no longer needed.

### Criteria (The way it should be)

Upon notification of an access change for a user account, the following user updates should occur:

1. Temporary access should be removed when no longer required.
- 2-4. Account maintenance of user access for database and application accounts needs to be performed to remove and/or disable accounts when no longer needed.

### Effect (So what?)

1. Excess user access remains available for users when no longer needed to perform their job responsibilities.
2. User activities and accountability may not be tied to one unique user account.
- 3-4. Potential misuse/abuse for active terminated user accounts may occur when not disabled in a timely manner.

### Cause (Difference between condition & criteria)

1. IT was not notified when temporary access was no longer needed.
2. Duplicate accounts were created due to a name change or unintentionally created.
3. A terminated account was missed in the termination account process.
4. A test account was not disabled when no longer needed.

### Recommendation

- 1.-4. Review the user administration management process periodically for the utility billing system to ensure that transfers, name changes (duplicates), terminations and test account are handled in a timely manner.

### Management Response

Management Concur.

### Action Plan

1. The temporary employee was not hired through the normal HR onboarding process. As a result, the temporary employee did not have a record in the HR employee management database. Since previous user access reports were created using the HR application as its source of city employees, temporary employees that were not part of the HR application were not accounted for. IT has now created a User Entitlement database to track all users of all applications and is maintained by IT. By use of this database IT will be able to account for temporary, contractor and all city employee application user accounts.
2. Duplicate accounts are created for various reasons (i.e. name changes). In

some cases a request is submitted to create a new account when an employee's name changes rather than to change the account name. IT evaluates requests in an effort to ensure that there is only one account in an application for any given employee. However, if a properly authorized "Account Creation Request" form is received and the form does not note that the request is a name change rather than a new account, it is possible that IT may create a new account. The User Entitlement review process is a mitigating control for this risk. Managing Directors or their delegates must review the User Entitlement report for accuracy to ensure an employee does not have more than one account.

3. ITS will ensure all terminated accounts are closed, disabled or deleted as appropriate.
4. Test accounts should not be used in production systems. Analyst will review their application users for any test accounts and remove them.

**Implementation Date**

Obj 1-2 May 2014

Obj 3-4 Dec 31 2013

## Finding #6 (Obj. 1)-ITS

### Condition (The way it is)

Twenty-four (24) terminated user accounts were still active on the Banner utility systems database server.

Note: The risk for the database accounts is lower as network access for these users were immediately disabled by IT upon notification by Human Resources.

### Criteria (The way it should be)

Periodic user account reviews should be performed for database and operating system accounts. Terminated user accounts should be removed in a timely manner.

### Effect (So what?)

Active widowed/orphaned accounts could potentially be misused.

### Cause (Difference between condition & criteria)

IT was not notified and/or the account management procedure to disable the accounts was not followed.

### Recommendation

1. IT should create a policy and procedure for a periodic review of operating system and database accounts for City systems.
2. Perform a quarterly/yearly review of operating system and database user accounts for appropriateness.

### Management Response

Management Concur.

### Action Plan

All database accounts are now part of the User Entitlement database tracking and as such will be disabled or deleted as appropriate once the termination ticket is issued. IT will more closely follow the database user account creation and deletion policy, which states these accounts will be reviewed on an annual basis. Any accounts other than user accounts (database, application user accounts) will be monitored separately as these are not tracked on User Entitlements.

### Implementation Date

May 2014

## **EXHIBIT A**

### **Reliability of Computer Generated Data**

#### **Banner Utility System Security Group Review (Obj. 1 & 2)**

1. IT generated a 457-page user list from the Banner utility application. The list provided the user, username and associated security groups. Within each security group a list of all application screens were included.

The reliability of computer generated data was reviewed by comparing the application generated report from Banner to the data extracted from ePersonality to Excel spreadsheets that were generated by IA to compare the access to other Banner security groups. The comparison focused on security groups or Customer Service and Cashier groups. Inquiry groups were not compared as the users have read only access.

We found that there is overlap of user access, but that it is provisioned due to a business need to provide adequate staff coverage for Customer Service job responsibilities. IA found the reliability of computer generated data to be accurate and complete.

2. IT generated a user report from the iNovah application during a meeting with IA. The users were compared to ePersonality to verify their job titles and active status. The users were verified and the data deemed reliable, but it should be noted that the iNovah application is not included in the annual user entitlement review.

#### **User Access Entitlement Report Review (Obj. 1 & 2)**

1. IT generated annual user access entitlement reports for all the Managing Directors.
2. The reliability of computer generated data was reviewed by comparing the IT generated report to IA generated reports generated using Crystal Reports by Organization number. We found 36 missing user accounts. IA did not find the reliability of the computer generated data to be reliable.

#### **User, system and service accounts (Obj. 1)**

1. IT generated a list of user, system and service accounts directly from the Banner and iNovah servers.
2. The reliability of computer generated data was reviewed for the completeness and accuracy of the user accounts, IA compared the Banner

and iNovah database user list to ePersonality to determine if they were active or inactive accounts. System and service accounts were reviewed and identified by IT and verified for their purpose.

We found the reliability of computer generated data to be accurate and complete.