CITY AUDITOR'S OFFICE

Selected Application Controls over the City's GenTax® System

SEPTEMBER 1, 2011 **AUDIT REPORT NO. 1209**

September 1, 2011

Honorable Mayor and Members of the City Council:

Enclosed is the audit report, *Selected Application Controls over the City's GenTax® System.* This system is used to process and manage information for transaction privilege (sales) tax, business and regulatory licensing, and alarm billing transactions and information.

The audit assessed the effectiveness of selected GenTax® application controls, specifically including those for system access and security management. Generally, there are sufficient procedures, reviews and reconciliations to identify and manage potential risks to the GenTax® system. However, certain changes can be made to user access rights and security parameters that will provide a higher level of assurance.

We would like to thank the staff from the Finance & Accounting and Information Technology divisions for their cooperation and assistance throughout the course of the audit.

If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

Sharron Walker

Sharron Walker, CPA, CFE
City Auditor

Audit Team:

Joyce Gilbride, CPA, CIA – Assistant City Auditor
Erika Keel, Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

An audit of Information Technology Controls of selected City information systems was included on the Council-approved fiscal year 2011/12 audit plan. For this audit, the Finance & Accounting Division's GenTax® application, which is used to manage the City's processes for transaction privilege (sales) tax, business and regulatory licensing, and alarm permit billing, was selected. The audit objective was to assess the effectiveness of GenTax® application-level controls, focusing on system access and security management.

The GenTax® application, which the City implemented about six years ago, primarily serves the Tax & License program within the Customer Service department. Tax & License uses the system to manage transactions and customer information and to generate tax returns, customer letters, and management reports. The Revenue Recovery program uses GenTax® to manage collections of delinquent tax and license accounts. Tax Audit uses GenTax® to research tax information and manage audits conducted on new and existing businesses. Additionally, various other City departments, such as Police and Transportation, have limited GenTax® access to review and approve their various regulatory licenses. GenTax® is supported by the Finance & Accounting Division, primarily through the services of a lead systems integrator and systems integrator who report to the Finance & Accounting Technology Director. According to the Finance & Accounting Technology Director, time spent by the two systems integrator positions supporting GenTax® is equivalent to 0.9 FTE. Assistance is also available from a vendor representative, who provides system updates and technical support when issues arise.

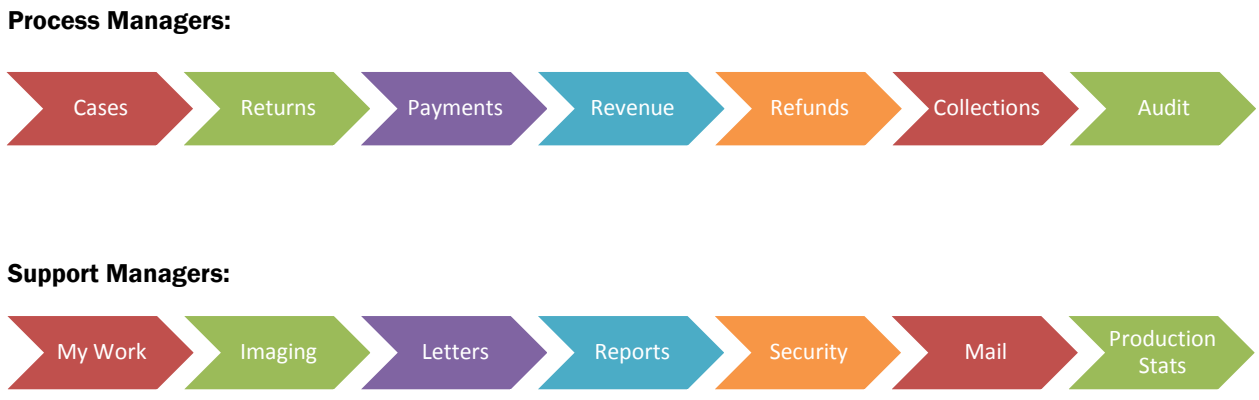
Generally, there are sufficient procedures, reviews and reconciliations to identify and manage potential risks to the GenTax® system. However, this established application is supported by experienced staff, so the processes and documentation that have been put in place are less formal. As a result, some improvements can be made to managing and documenting user access rights. Currently, there is limited documentation and policy on granting, changing, and revoking access. In addition, several users have more access than needed to accomplish their job duties, including six users who inappropriately have system administrative rights and one employee who can process refund transactions of any dollar amount from beginning to end. Further, system security can be improved through prohibiting shared user IDs, periodically reviewing user activity logs, strengthening passwords and periodically monitoring system functions and critical changes made to customer accounts.

BACKGROUND

In 2005, the City of Scottsdale selected and implemented GenTax® for the City's tax and licensing software. GenTax® is used to manage the City's processes for transaction privilege (sales) tax, business and regulatory licensing, and alarm permit billing. The flexibility of the system allows the City's technical staff to customize GenTax® to meet user needs and changes in the City's tax code and ordinances.

As shown in Figure 1 below, GenTax® divides information and/or processes into specific "Managers." Security is customizable to restrict user access to specific Manager(s). For example, through the Refund Manager a user may be able to change, approve, deny, void, re-issue, or reverse a refund, but is limited to only being able to view information in the Audit Manager. As the primary system user, Tax & License manages its tax and licensing work items, such as issuing licenses and updating customer information, and generates tax returns, customer letters, and management reports using the system. GenTax® is also used by other City functions. The Revenue Recovery program uses the system to manage collections of delinquent tax and license accounts. Tax Audit utilizes GenTax® to research tax information and manage audits conducted on new and existing businesses. And various other City departments, such as Police and Transportation, have limited GenTax® access to review and approve their specific types of regulatory licenses.

Figure 1. GenTax® Managers



SOURCE: Auditor analysis based on inquiry with GenTax® system administrators.

The GenTax® application, which resides on the City's network, is primarily maintained by the Finance & Accounting Division. This staffing includes a lead systems integrator and a systems integrator who report to the Finance & Accounting Technology Director. According to the Finance & Accounting Technology Director, his role is to provide management and contract oversight and the two systems integrators provide system support equal to 0.9 FTE. Assistance is also available from a vendor representative, who provides system updates and technical support when issues arise.

Information technology controls are those internal controls that are dependent on information system processing and include general controls and application controls.

General Controls are the policies and procedures that apply to all or a large segment of an entity's information systems to help ensure their proper operation. These controls include such standards as user authorization, configuration management, and contingency planning that serve to safeguard data, protect application programs, and ensure continuity of computer operations.

Application Controls are the policies and procedures to help ensure the proper operation of a specific business application, such as GenTax®. This type of controls can be further classified into application-level general controls (sometimes referred to as application security controls), business process controls, interface controls, and data management controls.

This audit reviewed the GenTax® application-level general controls, focusing on system access and security management. Guidance for testing information system controls is available from well-established audit organizations, including the Information Systems Audit and Control Association (ISACA) and the U.S. Government Accountability Office (GAO). The ISACA is an independent, nonprofit, professional organization that develops auditing and control guidance for information governance, security and audit professionals. The GAO is an independent nonpartisan agency that works for Congress, investigating how the federal government spends taxpayer dollars. In addition, the Internal Revenue Service has developed a Computer Security Evaluation Matrix specific to the GenTax® system that includes guidance on testing system access and security management.

OBJECTIVES, SCOPE, AND METHODOLOGY

An audit of Information Technology (IT) Controls was included on the Council-approved fiscal year 2011/12 audit plan; the City's GenTax® system was selected for this audit. As described in the Background, IT controls are considered at two levels: *general controls,* which relate to the overall operating environment, and *application controls,* which directly relate to the specific program or system. The audit objective was to assess the effectiveness of GenTax® system's application-level general controls over system access and security management. This Office's recent audit of IT controls for the TotalHR system also included a review of application-level general controls over change management. However, because the City's IT Division is currently implementing a City-wide change management system, the design and effectiveness of these controls for the GenTax® system was not included in the scope of the current audit.

To gain an understanding of the GenTax® system's application-level general controls, we interviewed key members of the Tax & License program and IT staff assigned to the Finance & Accounting Division who use or support the system regarding their processes and reviews. We also reviewed the written Tax & License program and Tax Audit policies and procedures to gain an understanding of how they use and monitor the GenTax® system. To gain an understanding of the described capabilities of GenTax®, we reviewed the Council Action Report dated January 25, 2005, requesting approval of the GenTax® system purchase as well as publicly available information regarding the system.

In designing tests of controls, we used the Information Systems Audit and Control Association's (ISACA) *IT Audit and Assurance Guidelines* G14, G38, and G40 related to system access and system security. We also used the U.S. Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual (FISCAM)* and the Internal Revenue Services' *Safeguard Computer Security Evaluation Matrix – GenTax®* in designing these tests. More specifically, we:

System Access
Reviewed the appropriateness of access levels based on the job function and job description of each authorized GenTax® user. This included a review for appropriate segregation of duties among the authorized users. In addition, we inquired about and tested the process for granting, reviewing, and revoking user access.

Security Management
Reviewed system security parameters, such as password strength, concurrent sessions, automatic timeouts, and number of user login attempts allowed. In addition, we inquired about system security training provided to GenTax® users and monitoring of user activity, especially regarding system administrators.

In addition to performing these procedures for our primary objectives, we reviewed the disaster recovery plan for GenTax®.

Based on audit work conducted, we concluded that there are sufficient procedures and reviews over system access and security management to identify and manage potential

risks to the GenTax® system. However, certain changes can be made to user access rights and security parameters that will provide a higher level of assurance

We conducted this audit in accordance with generally accepted government auditing standards as required by Article III, Scottsdale Revised Code, §2-117 et seq. 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. Audit work took place from mid-June through mid- August 2011, with Joyce Gilbride and Erika Keel conducting the work.

FINDINGS AND ANALYSIS

1. Several users have more system access than needed and authorization processes can be improved.

GenTax® users with critical roles are experienced and management has relied on this in operating with a less formal structure. However, in the following areas, system access can be improved.

A. Half of 28 sampled GenTax® users had system access levels exceeding their day-to-day job functions.

Each authorized GenTax® user is assigned to specific security groups, which have certain associated 'functions'. These functions provide the user with system access rights to the various Managers noted in Figure 1. These rights may be action-oriented, such as view, data entry, update, or approval, or may define types of transactions or data the user can see within a Manager, such as alarm permits or business licenses. However, documentation is not readily available and GenTax® system administrators were not able to readily define the access being granted through each security group or function. Based on the limited vendor documentation, inquiries and observations of the system, we developed general definitions of the access being provided for comparison to job responsibilities of a sample of authorized users. We selected 28 of the 63 authorized GenTax® users as of June 23, 2011, including all system administrators, to review the reasonableness of system access.

As shown in Table 1 below, at least 14 of these 28 users had more system access than necessary, with a majority being within the Tax & License program. Some employees' access to GenTax® has not been based on their regular job responsibilities and the principle of least privilege access.[1] In addition, users have multiple, sometimes redundant security groups assigned due to their access not being based on the principle of role-based access.[2] This allows a user to be assigned to the appropriate role, which simplifies the granting and review process and limits potential risk exposure.

Table 1. Users Access Levels

	Tax & License Users	Other Users	TOTAL	%
Unwarranted Access Level*	10	4	14	50%
Appropriate Access Level	7	7	14	50%
TOTAL	**17**	**11**	**28**	**100%**

* Access to functions and/or data not necessary for the user to accomplish their day-to-day duties.

SOURCE: Auditor analysis of job descriptions stated at City's HR website and users' security groups provided by GenTax® System Administrator.

[1] Least privilege access refers to providing only the system access necessary to perform one's job duties.

[2] Role-based access refers to assigning necessary access (i.e. least privilege) to specific roles or security groups and then assigning system users to the roles or groups.

Currently, four authorized GenTax® users have been established as system administrators with full system administrator access rights. In addition, at least five other users also have been granted some system administrator access rights. Six of these nine employees do not have regular responsibilities that would require such access. Because system administrator access provides powerful authority over the application, this level of access should be limited to the fewest employees possible. Additionally, three other authorized users inappropriately have the ability to write off financial transactions in the GenTax® system, and another user can view refund information, which is not necessary for his regular duties.

B. Some user access does not appropriately separate incompatible duties in GenTax®.

One individual currently has system access to initiate, review, and authorize refund checks of any dollar amount. Four management-level employees have system access that allows them to enter and update various tax and license account information, although this is not part of their regular job duties. Additionally, certain non-Tax & License users have system access to create a new license although that ability is incompatible with their regular function. Further, the Tax & License manager is not notified of any new licenses they establish in GenTax® to allow review for appropriateness and completeness of the license transaction.

The "segregation of duties" principle provides that key duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be separated so that one individual cannot process a transaction from beginning to end. This principle also applies to information systems. A formal segregation of duties analysis has not been performed for the GenTax® system.

C. Limited records have been kept of system user access authorizations, changes, and review.

The system administrators grant GenTax® access based on authorization from Tax & License management. This authorization most often comes in the form of an email request. These emails or other documentation supporting system access being provided, changed, or removed are not consistently kept. Only 5 of the 63 authorized GenTax® users had documented approval by appropriate management with the business purpose of their access level noted.

Because system access changes are not being tracked over time, we were unable to test the timeliness of access being revoked when authorized system users left City employment or changed jobs within the City. During the audit, one user resigned from the City and his/her system access was removed in a timely manner. However, we noted two authorized system users who had changed job positions and no longer needed access but had not been revoked. During the audit, access for these two users was removed.

According to the GenTax® system administrator, authorized users' system access has not been reviewed since implementation of GenTax® in November 2005. As shown in Table 2, eleven of the 63 authorized GenTax® user IDs, or 17%, have been inactive for a year or more. One user ID has been inactive for more than 37 months. During

the audit, access was also removed for these inactive users.

Table 2. Inactive User IDs

Length of Time	# of User IDs	% of User IDs
> 4 years	2	3%
2-3 years	3	5%
1-2 years	6	9%
Less than 1 year	52	83%
TOTAL	**63**	**100%**

SOURCE: Auditor analysis of last login date stated on June 23, 2011, user listing provided by GenTax® system administrator.

Periodic review of authorized users' system access is essential to ensuring the principle of least privilege access and timely removal of inactive or terminated employees. Effective user access reviews would require the managers who have requested GenTax® access for their staff to determine whether that access remains appropriate given any changes in job responsibilities.

Recommendations:

The Customer Service Director and Finance & Accounting Technology Director should:

A. Develop a written policy and procedures to govern GenTax® system access. This includes establishing role-based security groups with appropriate functions for each group of employees or third-parties based on their job duties and the "least privilege" principle. Then, using these defined security groups, perform a documented review of the appropriateness of each GenTax® system user's access. Reduce the number of system administrators to the fewest possible.

B. While establishing role-based security, also complete a segregation of duties analysis to ensure that one person cannot initiate, review, authorize, and complete a transaction from beginning to end in GenTax®.

C. Develop a written policy and procedures for granting, changing, and revoking user access. This should also include periodically reviewing authorized users' system access for reasonableness. For authorized users in other departments, their managers should be provided details on their granted access levels and asked to certify whether the specified system access is commensurate with current business needs and job duties.

2. Certain adjustments can better protect GenTax® data and business processes.

While this audit was not intended to review how GenTax® system changes are managed, a related issue became apparent during our work. As well, various security measures, such as user monitoring and password parameters, can be brought into better conformance with information security best practices.

A. Although a "Mail Forms" indicator appeared to be switched off on 64 accounts, the majority of these accounts continued to receive tax returns and other system generated mailings. Under certain circumstances, such as during a tax audit, City

staff suspends GenTax® system-generated mailings to the taxpayer to avoid duplication and minimize confusion. While testing whether mailings to the 64 accounts were turned off for appropriate reasons, we learned that management had recently discovered the mail indicator was not effective. The accounts were continuing to receive system-generated mail.

Apparently when the system was updated in 2009, this function was not tested to ensure that it properly suppressed system-generated mail. Information requested for this audit prompted management to discover this malfunction. Testing system functions and any system updates or changes is necessary to ensure that intended results are occurring.

B. While the system generally has good security controls, certain features can be improved. Currently, GenTax® user activity logs are not proactively monitored. In addition, improvement can be made in controls over password parameters, user ID requirements and user login attempts. The GenTax® system has customization features that allow stronger controls to be implemented. These issues have been discussed more specifically with management and are not detailed in this public report.

Recommendations:

The Customer Service Director and Finance & Accounting Technology Director should:

A. Work together to monitor system functions and critical changes made to customer accounts in GenTax®, such as stopping all mailings, for effective operation and continued appropriateness.

B. Consider strengthening security controls, as discussed more specifically with management.

MANAGEMENT RESPONSE

The GenTax Platform is a large, complex system designed to be flexible enough to meet the needs of nearly any jurisdiction in taxation and licensing. It is commonly employed by parishes, counties, states, and even national level agencies to manage these functions.

The City of Scottsdale obtained the platform in 2004/2005 in a competitive bidding process and completed implementation of the system in 2005/2006. The platform replaced two major, vendor unsupported systems. The promise of the platform was the ability for the City of Scottsdale to be able to make alterations and enhancements to the system without significant vendor support to meet the evolving needs of the city in taxation, regulatory licensing, and alarm billing management.

When the City procured the system it understood that sufficient staff would need to be dedicated to the system to maintain and enhance it. In the last three years staffing resources have gone from two FTE at implementation down to less than 1 FTE dedicated to the system due to increased workloads and staffing reductions. This reduced resource allocation is evident in day to day challenges in managing the system and in the audit findings.

In performing this audit, Internal Audit made use of several IT auditing and performance standards. While the City adheres to many of the elements within the myriad of standards utilized in this audit, we do not have the resources (human or financial) to adopt these in their entirety.

Information Technology Management would be happy to work with Internal Audit to develop an agreed upon adapted standard that is within our resource means.

MANAGEMENT ACTION PLAN

1. Several users have more system access than needed and authorization processes can be improved.

A. Half of 28 sampled GenTax® users had system access levels exceeding their day-to-day job functions.

Recommendation: The Customer Service Director and Finance & Accounting Technology Director should develop a written policy and procedures to govern GenTax® system access. This includes establishing role-based security groups with appropriate functions for each group of employees or third-parties based on their job duties and the "least privilege" principle. Then, using these defined security groups, perform a documented review of the appropriateness of each GenTax® system user's access. Reduce the number of system administrators to the fewest possible.

MANAGEMENT RESPONSE:

Management agrees that formalized policies, increased security documentation, and reducing administrator level access to the fewest needed will improve the overall management of the GenTax platform.

The GenTax platform's security is implemented today using a multi-layer security architecture. At the first layer is our City Standard domain security model which issues a single user account to each individual that requires a complex password. This user account is placed into a security group that enables select user access to the GenTax login screen. The second layer of security utilized groups or roles within the GenTax platform. These groups are configured with specific access to one or more of the 1,100+ functions or security points within the GenTax platform. This model is used by counties, states, and small countries around the world that employ the GenTax platform.

As Scottsdale has acquired, deployed, and updated the platform since 2005, our standard documentation has become less relevant. As such we can improve that documentation around security and roles to increase the transparency of the security model to enable better understanding of the security model. Due to the size and complexity of the model, this will be a resource consuming effort and will take some time to complete.

PROPOSED RESOLUTION:

Management will author security access and management polices to specifically apply to the GenTax platform.

Management will examine refining the security model to enable a more role centric structure to decrease the complexity of managing user security.

Management will examine the general system users to determine the most appropriate security group/role to place them in to ensure they have the appropriate access needed to perform their function.

Management will examine the users with administrative rights and work with the vendor

to find alternatives to enable key users to perform high security functions without administrative access when possible.

RESPONSIBLE PARTY:

Finance and Accounting Technology Director, Customer Service Director, Tax and License Manager

COMPLETED BY:

Projected June 2012

B. Some user access does not appropriately separate incompatible duties in GenTax®.

Recommendation: The Customer Service Director and Finance & Accounting Technology Director should while establishing role-based security, also complete a segregation of duties analysis to ensure that one person cannot initiate, review, authorize, and complete a transaction from beginning to end in GenTax®.

MANAGEMENT RESPONSE:

Management agrees that a segregation of duties analysis is warranted to highlight any area where a single user has end to end authorization authority and agrees to examine the appropriateness of that authority in context with the business structure and systems architecture.

The architecture of platforms such as GenTax will always enable a single user, most commonly the system administrator, to be able to perform all actions in the platform. While there are technical approaches that one can take to mitigate this, in our environment where we have very limited, often one, staff member who functions as the system administrator, it is not feasible.

When talking about standard user accounts, the segregation of key duties is possible with some additional configuration to the platform. Historically platforms such as GenTax are configured to allow a key employee, such as a business process manager, to have the ability to override an approval process as a safety valve in the system, commonly needed when upper level staff is unavailable and authority has been delegated to the business process manager. Management will work to identify an alternative approval process that will improve security without compromising system flexibility.

PROPOSED RESOLUTION:

Management will examine the duties and security of staff to ensure that that one person cannot initiate, review, authorize, and complete a transaction from beginning to end in GenTax with the exception of limitations imposed by the business structure or technical architecture of the platform.

RESPONSIBLE PARTY:

Finance and Accounting Technology Director, Customer Service Director, Tax and License Manager

COMPLETED BY:

Projected June 2012

C. Limited records have been kept of system user access authorization, changes, and review.

Recommendation: The Customer Service Director and Finance & Accounting Technology Director should develop a written policy and procedures for granting, changing, and revoking user access. This should also include periodically reviewing authorized users' system access for reasonableness. For authorized users in other departments, their managers should be provided details on their granted access levels and asked to certify whether the specified system access is commensurate with current business needs and job duties.

MANAGEMENT RESPONSE:

Management agrees that it can enhance its security review process to enable it to be more transparent and auditable.

Internal Audit has requested that we enhance our security authorization process to include additional details in our authorization process. Historically email requests from authorized personnel (or other equivalent documentation) has been considered acceptable authorization to grant access to the platform. Going forward we'll revise our security access process to provide the level of detail requested by Internal Audit to enable in subsequent audits a higher level of transparency.

PROPOSED RESOLUTION:

Management will author a written policy on security access and security review to provide enhancements to the current processes to enable a higher level of oversight and review.

RESPONSIBLE PARTY:

Finance and Accounting Technology Director, Customer Service Director, Tax and License Manager

COMPLETED BY:

January 2012

2. Certain adjustments can better protect GenTax® data and business processes.

Recommendations: The Customer Service Director and Finance & Accounting Technology Director should:

A. Work together to monitor system functions and critical changes made to customer accounts in GenTax®, such as stopping all mailings, for effective operation and continued appropriateness.

B. Consider strengthening security controls, as discussed more specifically with management.

MANAGEMENT RESPONSE:

The City of Scottsdale is moving to a new Information Technology Service Management platform later this calendar year that will enable a more consistent change management approach for systems overall. This new platform will help resolve some of the documentation and process concerns noted by Internal Audit.

As noted in the Audit a system flag that prevents mailings from being sent to certain customer accounts was not functioning as desired in the system. This element was tested and certified functional after the last systems upgrade by system testers. Unfortunately, testers can miss certain elements in testing due to the human involvement. In IT, when these situations occur we commonly augment the test scripts for the component in question to include additional testing for the system error or "bug".

It's possible to reduce the human interaction in the testing process by utilizing automated testing platforms such as IBM Rational, TestDrive, or QF-TEST, however the resources required to purchase and implement such solutions are beyond our current means.

Management does not see any needed changes in the standard testing process beyond enhancing the test scripts for this element or any other element in this scenario.

The GenTax system logs a significant amount of information on each action taken in the platform. The volume and complexity of the log data combined with less than 1 FTE assigned to the platforms full time management makes it very difficult to proactively review the logs while still meeting the day to day administration, business mandated, changes, council mandated changes, Arizona legislature mandated changes, and as well as general troubleshooting.

Management agrees that proactive monitoring of logs would be optimal security management; however the limited human resources make that difficult to do. If additional human resources can be provided or Internal Audit would like to become involved with that process we can pursue this endeavor.

The GenTax system has several options for its secondary user security. As noted even stronger controls can be implemented. To address several concerns from Internal Audit we will explore altering the security model to leverage the Active Directory security system which

would default the security to the core network security, thereby removing the secondary layer of security. This would then ensure the system meets the standards of the core network, automatically disable users that have left the City, and remove the need for several of the users to have system administration accounts that were performing password reset functions for the GenTax user population.

Management agrees that while very strong at present, the GenTax security controls can be made stronger.

PROPOSED RESOLUTION:

Management will seek additional human resources to support the GenTax platform to enable proactive review of the audit logs.

Management will explore implementing true Active Directory Integration for user security to ensure consistent user security standards.

RESPONSIBLE PARTY:

Finance and Accounting Technology Director

COMPLETED BY:

December 2011

City Auditor's Office
4021 N. 75th St., Suite 105
Scottsdale, Arizona 85251
(480) 312-7756
www.ScottsdaleAZ.gov/departments/City_Auditor

The City Auditor's Office provides independent research, analysis, consultation, and educational services to promote operational efficiency, effectiveness, accountability, and integrity in response to City needs.